SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 11 November 2026

Generated on 11 November 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-2026-123966	A vulnerability was determined in Tenda AC19 16.03.10.07. Affected by this issue is the function saveParentControlInfo of the file /goform/saveParentControlInfo. This manipulation of the argument deviceId causes heap-based buffer overflow. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	10.0	More Details
CVE-2026-121606	A vulnerability has been found in Qihoo 360 D621-2, D603-2, D600-2, D619, D606-6 and D706 up to 6.4.9. Affected by this issue is the function verify_sign of the file fs2/bin/iscm of the component Firmware Signature Verification. Such manipulation of the argument sign leads to improper verification of cryptographic signature. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	10.0	More Details
CVE-2026-122013	A vulnerability was detected in Comfast CF-WR632AX 2.6.0.1. Affected by this vulnerability is an unknown functionality of the file /usr/bin/webmgnt of the component Multipart Parser. Performing a manipulation of the argument filename results in path traversal. It is possible to initiate the attack 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.	10.0	More Details
CVE-2026-121933	A flaw has been found in Linksys E5350 1.0.00.037. This impacts the function save_settings of the file /wizard/apply.cgi of the component Setup Wizard. Executing a manipulation of the argument wizard_router_pwd can lead to missing authentication. The attack may be launched remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	10.0	More Details
CVE-2026-121932	A vulnerability was detected in Linksys E5350 1.0.00.037. This affects the function system of the file /wizard/apply.cgi. Performing a manipulation of the argument ping_ip/traceroute_ip results in os command injection. The attack may 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.	10.0	More Details
CVE-2026-121615	A vulnerability was determined in Linksys E5600 1.1.0.26. Affected is an unknown function of the file /cgi-bin/mesh_login.cgi of the component Login Handler. Executing a manipulation can lead to improper authentication. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way. This vulnerability only affects products that are no longer supported by the maintainer.	10.0	More Details
CVE-2026-121609	A vulnerability was identified in Qihoo 360 Whole Home Router M5 4.0.17.1566. This issue affects the function Home of the file /etc/init.d/mpt of the component Boot Script. The manipulation leads to hard-coded credentials. Remote exploitation of the attack is possible. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	10.0	More Details

CVE-2026-121607	A vulnerability was found in Qihoo 360 D603-2, D600-2, D606-6 and D706 up to 6.4.9. This affects the function testspeed_command of the file /fs2/bin/iscm. Performing a manipulation of the argument host results in os command injection. The attack may be initiated remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	10.0	More Details
CVE-2026-122051	A flaw has been found in Edimax BR-6208AC 1.32. Affected by this vulnerability is an unknown functionality of the file /goform/mp. Executing a manipulation can lead to command injection. The attack may be launched remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	10.0	More Details
CVE-2026-109469	Authorization bypass through user-controlled key in Entra Device Registration allows an unauthorized attacker to elevate privileges over a network.	10.0	More Details
CVE-2026-118423	The WP Libre Form WordPress plugin 1.5.0.1 does not validate the type of files uploaded through its form submissions, allowing unauthenticated attackers to upload PHP files to a web-accessible location and execute them, leading to remote code execution.	10.0	More Details
CVE-2026-71495	Wanderer is a self-hosted trail database for saving and sharing adventures. Prior to 0.20.0, when PUBLIC_PRIVATE_INSTANCE is not set to true, the unauthenticated POST /api/v1/trail/download handler passes the attacker-controlled JSON url field directly to event.fetch() and returns the fetched response. This allows requests to internal services such as db:8090 and search:7700, cloud metadata addresses, and other network destinations, exposing returned data and permitting internal network reconnaissance or denial of service. This issue is fixed in version 0.20.0.	10.0	More Details
CVE-2026-16884	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote attacker to obtain sensitive information due to an XML external entity (XXE) injection.	9.9	More Details
CVE-2026-17298	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to server-side request forgery.	9.9	More Details
CVE-2026-122303	Kyverno from 1.17.0 before 1.19.2 contains an authorization bypass vulnerability that allows namespace tenants to overwrite resources in other namespaces via NamespacedMutatingPolicy mutate-existing targetMatchConstraints.expression. Attackers can return a CEL map literal fabricating a target with an attacker-chosen metadata.namespace, causing the privileged background controller to overwrite Secrets, Deployments, or policies cluster-wide.	9.9	More Details
CVE-2026-122304	Kyverno from 1.17.0 before 1.19.2 contains an authorization bypass vulnerability that allows namespace admins to escape namespace confinement because the cleanup controller builds its context loader with a nil policy. Attackers can create a namespaced CleanupPolicy with apiCall or globalReference context entries to read cross-namespace Secrets and modify validatingwebhookconfigurations using the cleanup controller's ServiceAccount.	9.9	More Details
CVE-2026-122310	Kyverno from 1.19.1 before 1.19.2 validates a Policy's context.apiCall urlPath after cleaning it but executes the raw path, whose fragment or query the Kubernetes client discards. A namespace-scoped user who can create a Policy can hide ../ segments behind # or ? to reach cluster-scoped endpoints with Kyverno's ServiceAccount, gaining cluster admin.	9.9	More Details
CVE-2026-122193	OS command injection in the example SSM document provisioning script in Trusted Remote Execution (REX) before 2026-07-28 might allow an authenticated remote user who is permitted to invoke the Rex-RO or Rex-RW SSM document to execute arbitrary commands as root on the managed instance, bypassing Cedar policy enforcement. To remediate this issue, users should delete any Rex-RO and Rex-RW SSM documents created from the example script, in each account and Region where it was run.	9.9	More Details
CVE-2026-122313	Kyverno from 1.17.0 before 1.19.2 contains a privilege escalation vulnerability that allows namespace-scoped tenants to modify resources in other namespaces through NamespacedMutatingPolicy targetMatchConstraints.expression CEL output lacking namespace checks. Attackers can emit a literal target such as another tenant's RoleBinding, which the cluster-wide background controller then mutates to add attacker subjects or alter Roles, NetworkPolicies, and ConfigMaps.	9.9	More Details
CVE-2026-17239	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to execute arbitrary code due to a path traversal vulnerability.	9.9	More Details
CVE-2026-17158	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to gain elevated privileges due to improper authentication.	9.9	More Details
CVE-2026-17150	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to execute arbitrary code and access sensitive information from other tenants due to insufficient input validation. Uploaded custom module content is not sufficiently validated before it is processed, which could allow code to run with access beyond the user's own tenant.	9.9	More Details
CVE-2026-17147	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to execute arbitrary code and perform unauthorized administrative actions due to a path traversal vulnerability.	9.9	More Details
CVE-2026-	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote		

17146	authenticated attacker to execute arbitrary JavaScript and obtain sensitive information due to improper input validation.	9.9	More Details
CVE-2026-17134	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to execute arbitrary SQL commands due to SQL injection.	9.9	More Details
CVE-2026-97693	Yuxi is a large-model-based intelligent knowledge base and knowledge graph agent development platform. From 0.6.0.beta1 until 0.7.1, there is insufficient isolation between execution-capable Docker sandboxes and trusted application services. A low-privileged authenticated user who can execute commands in their own sandbox can reach other tenants' sandbox APIs, access their files and secrets, execute commands in active sandboxes, and enumerate, create, or delete sandboxes through the unauthenticated provisioner without knowing administrator, database, or MinIO credentials. Sandboxes can also reach shared internal services; if shipped default service credentials remain unchanged, an attacker can use them, and if the exposed PostgreSQL account is a superuser, obtain command execution in the PostgreSQL container. These paths can disclose or modify cross-tenant data and sandbox state or cause denial of service through sandbox deletion without a container escape or kernel vulnerability. This vulnerability is fixed in 0.7.1. Existing deployments must separately rotate persisted PostgreSQL, Neo4j, or MinIO credentials that were previously set to documented or shipped defaults because upgrading the Compose files does not automatically rotate them.	9.9	More Details
CVE-2026-17117	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to execute arbitrary code due to improperly controlled modification of object attributes. A user could set a field that should only be controlled by the system, which could lead to code execution.	9.9	More Details
CVE-2026-17049	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information and modify arbitrary documents due to authorization bypass through user-controlled keys.	9.9	More Details
CVE-2026-16920	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to bypass security restrictions due to a confused deputy vulnerability.	9.9	More Details
CVE-2026-71550	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to 7.15.2 and 8.10.2, the workflow controller uses a path-traversal-capable aow_action value in require_once() without constraining the resolved file. The affected flow begins at modules/AOW_WorkFlow/controller.php and uses aow_action, and require_once() to carry attacker-controlled data or authorization state into the security-sensitive operation. An authenticated user with the WorkFlow role can include executable PHP, obtain server-side code execution, access CRM data and configuration secrets, and establish persistent access. This issue is fixed in versions 7.15.2 and 8.10.2.	9.9	More Details
CVE-2026-17132	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to execute arbitrary SQL commands due to improper neutralization of special elements used in an SQL command.	9.9	More Details
CVE-2026-122311	Kyverno from 1.16.0 before 1.19.2 fails to validate path segments in the resource argument of resource.get() and resource.post(), allowing namespaced CEL policies to escape their namespace. Tenants who can create a NamespacedValidatingPolicy can insert .. segments to read and write arbitrary cluster objects using the admission controller's ServiceAccount, leading to cluster takeover.	9.9	More Details
CVE-2026-17336	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to execute arbitrary SQL commands due to improper neutralization of special elements used in an SQL command.	9.9	More Details
CVE-2026-17399	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to execute arbitrary code due to insufficient validation of uploaded content. Content uploaded to the product is not sufficiently checked before it is processed, which could allow code to run on the server.	9.9	More Details
CVE-2026-121599	A vulnerability was detected in TOTOLINK A950RG 4.1.2cu.5268_B20221104. Affected is the function setWiFiMultipleConfig/delWiFiMultipleConfig of the file /cgi-bin/cstecgi.cgi of the component Multi-SSID Configuration. The manipulation of the argument wepkey2/wepkey3 results in stack-based buffer overflow. It is possible to launch the attack remotely. The exploit is now public and may be used.	9.9	More Details
CVE-2026-121598	A security vulnerability has been detected in TOTOLINK A950RG 4.1.2cu.5268_B20221104. This impacts the function strcpy of the file /cgi-bin/cstecgi.cgi of the component Basic Wireless Configuration Handler. The manipulation of the argument wepkey leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used.	9.9	More Details
CVE-2026-121597	A weakness has been identified in TOTOLINK A950RG 4.1.2cu.5268_B20221104. This affects the function setAppEasyWizardConfig of the file /cgi-bin/cstecgi.cgi of the component Easy Setup Wizard Handler. Executing a manipulation of the argument functionType can lead to stack-based buffer overflow. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks.	9.9	More Details
CVE-2026-121600	A flaw has been found in TOTOLINK A950RG 4.1.2cu.5268_B20221104. Affected by this vulnerability is the function setMacFilterRules of the file /cgi-bin/cstecgi.cgi of the component MAC Filter Handler. This manipulation of the argument addEffect causes stack-based buffer overflow. The attack can be initiated remotely. The exploit has been published and may be used.	9.9	More Details

CVE-2026-123961	A security vulnerability has been detected in TOTOLINK CA300-PoE 6.2c.884. This impacts the function setWiFiBasicConfig of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument KeyStr leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used.	9.9	More Details
CVE-2026-123960	A weakness has been identified in TOTOLINK CA300-PoE 6.2c.884. This affects the function setWanConfig of the file /cgi-bin/cstecgi.cgi. Executing a manipulation of the argument pppoeUser/priDns/secDns can lead to buffer overflow. The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks.	9.9	More Details
CVE-2026-123958	A vulnerability was identified in TOTOLINK CA300-PoE 6.2c.884. The affected element is the function setLanConfig of the file /cgi-bin/cstecgi.cgi. Such manipulation of the argument lanDns/lanSecDns/langType leads to buffer overflow. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	9.9	More Details
CVE-2026-17410	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to access and modify other tenants' portal data due to improper neutralization of argument delimiters.	9.9	More Details
CVE-2026-17402	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to execute arbitrary commands due to OS command injection. User-supplied input is not properly neutralized before it is passed to the operating system, which could allow commands to run on the underlying host.	9.9	More Details
CVE-2026-123957	A vulnerability was determined in TOTOLINK CA300-PoE 6.2c.884. Impacted is the function setIpQosRules of the file /cgi-bin/cstecgi.cgi. This manipulation of the argument ipStart causes buffer overflow. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.	9.9	More Details
CVE-2026-17354	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to perform arbitrary file writes due to path traversal.	9.9	More Details
CVE-2026-17392	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to gain unauthorized administrative access to other tenants due to LDAP injection. User-supplied input is not properly neutralized in directory queries, which could change the query and grant access beyond the user's own tenant.	9.9	More Details
CVE-2026-17359	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to execute arbitrary code due to improper control of generation of code. A user-supplied value can influence code that the product generates, which could lead to code execution.	9.9	More Details
CVE-2026-17342	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to execute arbitrary code due to improper control of generation of code.	9.9	More Details
CVE-2026-121265	SQL::Abstract versions before 2.000003 for Perl allow SQL injection via an arrayref column value in insert and update. With the array_datatypes option off, which is the default, insert(), update() and values() treat an arrayref column value as literal SQL. Its first element goes into the SQL text unescaped and the rest become bind values. A JSON array, or a repeated form field decoded as an arrayref, is such a value. An application that passes request data as column values to insert or update with the default options allows SQL injection. Releases before 2.000003 also treat an arrayref in generate() as literal SQL, including through AUTOLOAD when allow_autoload is on, whatever array_datatypes is set to.	9.8	More Details
CVE-2026-58490	Tracecat is an open-source security automation platform for teams and AI agents. From version 0.37.0 until 1.0.0-beta.49, Docker Compose deployments with SAML enabled can render SAML_SIGNED_ASSERTIONS and SAML_SIGNED_RESPONSES as empty values, overriding secure application defaults and disabling both signature requirements. An unauthenticated attacker who can reach the SAML assertion consumer endpoint can submit a forged unsigned response for an existing Tracecat user email address and obtain that user’s session. Targeting an existing superadmin can result in superadmin account takeover. Exploitation does not create users when SAML user creation is disabled and does not affect default Fargate or Helm deployments. Version 1.0.0-beta.49 removes the insecure deployment pass-through and requires signed assertions and responses.	9.8	More Details
CVE-2026-123776	RRD::CGI::Image versions through 0.01 for Perl pass CGI query parameters containting "tz" to tzset(), , so a FIFO or device path blocks the CGI process. The normalize_params method sends any query key matching /tz/i to tz(), which sets $ENV{TZ} to that value, with no validation. It then calls tzset(). glibc treats a TZ value starting with / or : as a file path and opens it, so a value naming a FIFO or a blocking device stalls the process inside tzset().	9.8	More Details
CVE-2026-119516	Deserialization of Untrusted Data vulnerability in Mamunur Rashid Radius Booking — Booking Calendar for Appointments & Services radius-booking allows Object Injection.This issue affects Radius Booking — Booking Calendar for Appointments & Services: from n/a through 1.0.20.	9.8	More Details
CVE-2026-84473	Authentication Bypass / Missing Brute-Force Protection in remote.php/webdav/ in ownCloud ownCloud server 10.16.3 allows an unauthenticated remote attacker to perform unlimited online password guessing against WebDAV accounts via repeated HTTP Basic Authentication requests to the WebDAV endpoint.	9.8	More Details
	A heap-based buffer overflow in the TDS prelogin parser in the Babelfish for PostgreSQL extension versions		

CVE-2026-119923	1.0-1.5, 2.1-2.15, 3.1-3.12, 4.0-4.8, 5.1-5.4 and in Amazon Aurora PostgreSQL with Babelfish might allow remote attackers to execute arbitrary OS commands as the database process user via a specially crafted malformed TDS prelogin packet to the TDS port. This record consolidates a related NULL-pointer-dereference finding in the same prelogin parser. To remediate this issue, we recommend users upgrade to Babelfish for PostgreSQL extension versions 4.10, 5.6, 6.1 or later. As a workaround, restrict network access to the TDS port (default 1433). Customers using Amazon Aurora PostgreSQL with Babelfish should upgrade their cluster to Aurora PostgreSQL 13.9.16 (1.5.5), 13.23.3 (1.17.2), 14.6.16 (2.3.5), 14.17.8 (2.12.4), 14.18.6 (2.13.3), 14.19.5 (2.14.2), 14.20.5 (2.15.2), 14.22.3 (2.16.1), 14.23.1 (2.17.0), 15.10.8 (3.8.4), 15.12.8 (3.9.4), 15.13.6 (3.10.3), 15.14.5 (3.11.2), 15.15.5 (3.12.2), 15.17.3 (3.13.1), 15.18.1 (3.14.0), 16.8.8 (4.5.5), 16.9.6 (4.6.3), 16.10.5 (4.7.2), 16.11.5 (4.8.2), 16.13.3 (4.9.1), 16.14.1 (4.10.0), 17.4.8 (5.1.4), 17.5.6 (5.2.3), 17.6.5 (5.3.2), 17.7.5 (5.4.2), 17.9.3 (5.5.1), 17.10.1 (5.6.0), 18.3.4 (6.0.2), 18.4.1 (6.1.0) or later, and apply any pending maintenance to ensure they are on the latest patch.	9.8	More Details
CVE-2026-76168	In Apache James server prior version 3.9.1 relying on the SieveFileRepository incorect validation of file paths can result in path transversal, allowing to set arbitrary SIEVE scripts for other users. This allows a logged in attacker to set arbitrary SIEVE scripts for other users, resulting in denial of service or even traffic capture. Users are recommended to upgrade to version 3.9.1 which fixes this issue.	9.8	More Details
CVE-2026-123488	Craft CMS 4.0.0 before 4.18.9 and 5.0.0 before 5.11.2 contains an unauthenticated SQL injection vulnerability in the element search endpoint because the attribute parameter is concatenated into the query unsanitized and emulated PDO prepares allow stacked statements. Remote attackers can read and write the database, setting the admin flag or overwriting password hashes in the users table to gain administrator access.	9.8	More Details
CVE-2026-90436	** UNSUPPORTED WHEN ASSIGNED ** Deserialization of an inbound SOAP fault in Apache Axis 1.x allows unauthenticated remote class instantiation. When a SOAP <Fault> carries a <detail><exceptionName> element, Axis loads the named class and, if a String <data> element is also present, instantiates it through its String constructor before checking that it is an AxisFault. Loading alone runs the class's static initializer. With a suitable class on the application's classpath this leads to remote code execution. The fault is parsed while the engine resolves the target service, before any per-service handler chain runs, so authentication handlers configured on a service do not protect against it. This affects all Apache Axis 1.x versions through 1.4. As Axis 1 has been EOL we recommend you migrate to a different SOAP engine, such as Apache Axis 2/Java. Alternatively you could use a build of Axis with the patch from https://github.com/apache/axis-axis1-java/commit/41f3b4e8d04e310ca81f86b92630ab2c11d608bd applied. The Apache Axis project does not expect to create an Axis 1.x release fixing this problem.	9.8	More Details
CVE-2026-59105	Jumis (formerly Tildes Jumis) creates and uses a Microsoft SQL Server login named ##Tilde_JumisAdmin## whose password is derived deterministically from a single non-secret input - the SQL Server name (@@servername). The derivation algorithm is hard-coded in the client application and is identical across every installation; it contains a hard-coded secret key for entropy. Because the only input (the server name) is not secret - the instance suffix is hard-coded and the host name is discoverable via the SQL Server Browser service (UDP 1434), the TDS pre-login response, or DNS/NetBIOS - any party able to reach a Jumis SQL Server can compute the password offline and authenticate. The ##Tilde_JumisAdmin## login is a member of the sysadmin server role. Successful authentication therefore grants full administrative control of the SQL Server instance and read/write access to every customer's accounting database hosted on it. The on-premise server installation also programmatically enables xp_cmdshell during routine operation, so sysadmin access escalates to operating-system command execution on the database server.	9.8	More Details
CVE-2026-120844	Incorrect Privilege Assignment vulnerability in miniOrange OAuth Single Sign On – SSO (OAuth Client) miniorange-login-with-eve-online-google-facebook allows Privilege Escalation.This issue affects OAuth Single Sign On – SSO (OAuth Client): from n/a through 7.1.3.	9.8	More Details
CVE-2026-107622	The BuddyForms plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 2.10.5 via a form-type confusion attack through the `bf_post_type` parameter. This is due to the public frontend submission handler `buddyforms_form_response_no_ajax()` authorizing logged-out submissions based solely on the target form's `public_submit` flag while independently trusting the attacker-supplied `$_POST['bf_post_type']` to determine the post type of the newly created object — a cross-check introduced in 2.10.2 applies only to existing posts (`post_id != 0`) and is completely bypassed for new-object creation — combined with the `save_post` listener `buddyforms_edit_form_save_meta_box_data()` lacking both a `current_user_can()` capability check and a form-builder nonce, causing it to unconditionally persist attacker-supplied `$_POST['buddyforms_options']` for any newly inserted `buddyforms` CPT post. This makes it possible for unauthenticated attackers to insert a rogue BuddyForms form configuration with an attacker-controlled `new_user_role` value into the live global form registry, then submit a registration through that form to create a new WordPress account with administrator-level privileges and achieve full site takeover. Exploitation requires the WordPress site to have "Anyone can register" enabled and at least one public BuddyForms form attached to a page, both of which are standard BuddyForms deployment configurations.	9.8	More Details
CVE-2026-63438	2FAuth is a web app to manage Two-Factor Authentication (2FA) accounts and generate their security codes. Prior to 8.0.0, when AUTHENTICATION_GUARD=reverse-proxy-guard accepts authentication headers from a client that did not pass through a trusted proxy, RemoteUserProvider::retrieveById() creates an account for an unknown REMOTE_USER, promotes the first created account to administrator, and synchronizes the account email from the configured mail header. An unauthenticated remote client can	9.8	More Details

	therefore create an administrator on a fresh instance or impersonate and redirect email for a known account, exposing 2FA secrets and administrative functions. This issue is fixed in version 8.0.0.		
CVE-2026-54349	Chartbrew is an open-source web application that can connect directly to databases and APIs and use the data to create charts. Prior to 5.2.1, SQL dashboard-variable substitution used attacker-controlled JavaScript replacement strings unsafely across SQL connectors and separately failed to escape backslashes for MySQL and MariaDB quoted contexts. The vulnerable surface is public and embedded dashboard/chart requests that call applyMysqlOrPostgresVariables. An unauthenticated user sends crafted URL filter values to a public or embedded chart backed by a stored SQL query. Replacement-string dollar sequences can alter SQL independently of the database engine, while MySQL and MariaDB backslash handling provides a second quoted-string escape path. The target must expose a public or embedded chart using URL-controlled variables in a SQL query; only the backslash branch is specific to MySQL and MariaDB. Injected SQL can read, modify, or delete data available to the configured database account. This issue is fixed in version 5.2.1.	9.8	More Details
CVE-2026-17362	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote attacker to create, modify, or delete tenants due to missing authorization.	9.8	More Details
CVE-2026-63439	2FAuth is a web app to manage Two-Factor Authentication (2FA) accounts and generate their security codes. Prior to 8.0.0, when AUTHENTICATION_GUARD=reverse-proxy-guard is enabled, ReverseProxyGuard::user() reads the default REMOTE_USER identity header, or a custom identity header selected by the AUTH_PROXY_HEADER_FOR_USER configuration setting, without confirming that the request originated from a configured trusted proxy. A remote client that can reach the application directly can forge the selected identity header and authenticate as an existing user, including an administrator, gaining access to stored 2FA secrets and account or application management functions. This issue is fixed in version 8.0.0.	9.8	More Details
CVE-2026-104014	The Naimur Email OTP Verification for WooCommerce plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 2.1.0. This is due to the plugin's password-reset finalization endpoint (the wp_ajax_nopriv_ceovw_update_new_password action handled by CEOVW_AJAX::update_new_password()) authorizing the reset solely by the presence of a database row marking an email as 'VERIFIED', with no timestamp check, no session binding, and no per-reset token — combined with mark_otp_as_verified_for_reset() leaving the row in that state after a user enters their code (abandoning the flow leaves the row behind), and a scheduled 'ceovw_cleanup_expired_otps_event' cron that has no add_action() handler anywhere in the plugin so cleanup never runs. This makes it possible for unauthenticated attackers to take over any account whose owner previously requested and verified a password-reset code and did not immediately finish choosing a new password — the attacker needs only the victim's email address and a nonce that the plugin itself localizes publicly into the CEOVW_APP global on the WooCommerce account page for logged-out visitors, after which they call the endpoint, overwrite the victim's password, and are returned a live wordpress_logged_in_ session cookie for that user (full site takeover if the account is an administrator).	9.8	More Details
CVE-2026-17301	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow an unauthenticated attacker to bypass authentication due to improper verification of a cryptographic signature.	9.8	More Details
CVE-2026-17340	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote attacker to execute arbitrary code due to a path traversal vulnerability.	9.8	More Details
CVE-2026-17360	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote attacker to gain full administrative control due to the use of hard-coded credentials.	9.8	More Details
CVE-2026-115230	The WHIZZ WordPress plugin through 1.1.8 does not validate the password-reset key before updating a user's password, relying only on a nonce that is exposed to unauthenticated visitors, allowing attackers to set an arbitrary password for any user, including administrators, and fully take over their accounts.	9.8	More Details
CVE-2026-17278	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote attacker to gain unauthorized access to sensitive API catalog and runtime configuration data due to improper authentication. Information supplied by the client is not sufficiently verified, which could allow a caller to appear as a trusted party.	9.8	More Details
CVE-2026-17408	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote attacker to execute arbitrary code due to improper neutralization of special elements in an OS command.	9.8	More Details
CVE-2026-119075	The Registration Form for WooCommerce plugin for WordPress is vulnerable to privilege escalation due to a missing allow-list check in the FormHandler::validate_checkout_fields() function in versions up to, and including, 1.1.4 The My Account registration path (validate_fields()) validates a submitted 'tgwcfb/user-roles' value against the form's configured allowed roles, but the checkout registration path (validate_checkout_fields(), hooked to woocommerce_after_checkout_validation) stores the raw $_POST['user_roles'] value in $this->valid_data without any allow-list enforcement, and add_user_data() then injects that value into woocommerce_new_customer_data as the new account's role. This makes it possible for unauthenticated attackers to elevate their privileges to Administrator by supplying a user_roles=administrator parameter when creating an account during checkout, resulting in full site takeover.	9.8	More Details

CVE-2026-85295	Chartbrew is an open-source web application that can connect directly to databases and APIs and use the data to create charts. Prior to 5.2.3, four authentication helpers accepted session tokens signed with CB_SECRET, including known, weak, or shipped-default values. The vulnerable surface is session JWT fallback in server/modules/verifyToken.js, verifyUser.js, getUserFromToken.js, and socketManager.js across the API and socket layer. A stock source or repository Docker Compose deployment retains a known, weak, or default CB_SECRET and an attacker submits a forged HS256 token decoding to a target user id. Knowing the symmetric secret lets the attacker create a token that the legacy verification fallback accepts as the target user without that user's password or two-factor authentication. The condition includes stock source and repository Docker Compose installs and any otherwise known or weak CB_SECRET; a bare container where CB_SECRET is undefined is not affected by this fallback path. A forged session impersonates the chosen user across the entire API and socket layer and exercises that user's Chartbrew privileges. This issue is fixed in version 5.2.3.	9.8	More Details
CVE-2026-16720	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote attacker to obtain valid access tokens for other users due to improper authentication. Authentication against a connected directory service is not sufficiently enforced, which could allow another user's identity to be assumed.	9.8	More Details
CVE-2026-19803	The Printcart Store – Web to Print Product Designer for WooCommerce plugin for WordPress is vulnerable to Arbitrary File Upload in all versions up to, and including, 2.13.2. This is due to the `nbu_crop_image` AJAX handler accepting a user-supplied `url` parameter that `Nbdesigner_IO::convert_url_to_path()` concatenates onto the uploads base directory without normalizing or stripping `../` sequences, and then deriving both the output directory and output file extension via `pathinfo()` from the same attacker-controlled path — with no `stripImage()` call before `writeImage()` is invoked. This makes it possible for unauthenticated attackers to write attacker-controlled PHP content to arbitrary locations outside the uploads directory, resulting in remote code execution when the written file is subsequently requested. This vulnerability is only exploitable when the `nbdesigner_upload_popup_style` site option is set to `a` (Advanced Upload Popup), which causes the handler to be registered for unauthenticated requests; however, the required `save-design` nonce is printed on the fully public frontend `upload-design-file` page, making it trivially obtainable by any anonymous visitor once that configuration is active.	9.8	More Details
CVE-2026-17313	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote attacker to obtain sensitive information and take control of gateway configuration due to authentication bypass via an alternate path.	9.8	More Details
CVE-2026-123218	IBM Aspera Faspex 5.0.0 through 5.0.19 could allow an authorized user to craft a specific message to bypass user authorization and gain full administrative privileges.	9.8	More Details
CVE-2026-93754	The payever – WooCommerce Gateway plugin for WordPress is vulnerable to arbitrary file upload leading to remote code execution in various versions up to, and including, 4.8.0. Three WooCommerce-API callbacks (payever_set_sandbox_api_keys, payever_toggle_subscription, payever_synchronization_incoming) are registered with no authentication, capability check, or nonce, and the upload_image() routine writes a remotely fetched file to the public uploads directory using an attacker-controlled basename() BEFORE validating the file type. This makes it possible for unauthenticated attackers to write an executable PHP file and achieve remote code execution. NOTE: the token-recovery leg of the full chain depends on the plugin's outbound validateToken() call to Payever's service; the unauthenticated hard-coded-credential identity overwrite (CWE-862/CWE-798) is independently exploitable.	9.8	More Details
CVE-2026-59104	UgCS server before 6.2 contains an authentication bypass in the HCI protocol login handler (LoginHandler) exposed on TCP port 3334. When the user database contains exactly one user (the default single-operator installation), a LoginRequest with empty userLogin and userPassword fields is interpreted as \"use the only user\" rather than as invalid credentials, and the server returns a fully authenticated session. Because the service listens on all interfaces (0.0.0.0) without TLS by default, an unauthenticated remote attacker with network access to port 3334 can obtain an authenticated session without knowing any credential and then issue privileged commands, including commanding connected drones and uploading flight routes.	9.8	More Details
CVE-2026-116533	The Static Snapshot WordPress plugin through 0.2.1 does not sanitise shell metacharacters in a user-supplied value before concatenating it into operating-system commands run by the server, allowing unauthenticated attackers to execute arbitrary commands on the host.	9.8	More Details
CVE-2026-120637	CGI versions before 5.00 for Perl take request parameters from the process command line arguments for an unrecognised REQUEST_METHOD. For a REQUEST_METHOD such as OPTIONS, CGI falls through to its offline debugging mode, which is on by default, and builds the parameters and path_info from the process's command line arguments.	9.8	More Details
CVE-2026-113615	The GS JWT Authentication for WP REST API WordPress plugin through 1.0.0 does not sanitize or parameterize a request value before using it in SQL queries on several unauthenticated REST routes, allowing unauthenticated attackers to perform SQL injection and obtain an administrator session.	9.8	More Details
CVE-2026-122302	Kyverno before 1.19.2 contains a privilege escalation vulnerability that allows namespace admins to create resources beyond their RBAC because generate-rule admission checks verify the controller's permissions, not the author's. Attackers can create a namespaced Policy with generate rules targeting other namespaces or cluster-scoped kinds, making the background controller create or clone resources cluster-wide.	9.8	More Details
	Improper Control of Generation of Code ('Code Injection') in Apache OFBiz 24.09 before 24.09.08 on all		

CVE-2026-83542	platforms allows a remote unauthenticated attacker to execute arbitrary code on the server by staging crafted widget XML in a multipart upload and overriding the mainDecoratorLocation used by a manager login route through an anonymous JSON request, causing OFBiz to load the staged XML through its live screen descriptor mechanism and evaluate an unsandboxed Groovy expression while rendering the authentication-failure page. Further validation established the following: -- The exploit does not require a malformed or incomplete multipart body: a well-formed multipart request that is kept in flight and then allowed to complete normally is sufficient. -- The screen loader reads the widget XML from a live process file descriptor while the upload is streaming, rather than from any file the attacker persists to disk. -- The same underlying issue is also reachable through the public, explicitly unauthenticated /sfa/control/editPortalPageColumnWidth route, returning command output directly in an HTTP 200 response — it is not limited to the login-failure rendering path used in the original report. Users are recommended to upgrade to version 24.09.08, which fixes this issue.	9.8	More Details
CVE-2026-82907	Authentication Bypass by Capture-replay in ExternalLoginKeysManager in Apache OFBiz 24.09 before 24.09.08 on all platforms allows a remote unauthenticated attacker who captures a live externalLoginKey value to obtain a complete, cookie-free, reusable session as the user who issued it, in every webapp that user can reach, because checkExternalLoginKey runs as a global preprocessor ahead of both the CSRF and authentication checks and accepts the key as a bearer credential that is never bound to a client, never expires, and is not invalidated after use, while the framework itself both appends live keys to every cross-webapp link it renders and, via WidgetWorker's unvalidated inter-app link target, lets an authenticated user's key be attached to an attacker-chosen absolute URL and delivered directly to the attacker's own server. Users are recommended to upgrade to version 24.09.08, which fixes this issue.	9.8	More Details
CVE-2026-105330	Use of Hard-coded Cryptographic Key in JWT token authentication in Apache OFBiz 24.09.06 and 24.09.07 on all platforms allows an unauthenticated, network-reachable attacker to obtain full administrative access via a forged JWT signed with the factory-default security.token.key value that CVE-2026-31986 removed from newly generated configurations, on a deployment that upgraded from a release predating that fix while retaining its existing security.properties with security.internal.sso.enabled set to true. Users are recommended to upgrade to version 24.09.08. Upgrading alone does not replace an already-configured key: deployments that carried framework/security/config/security.properties forward from a release predating the CVE-2026-31986 fix must also run './gradlew rotateSecretKeys' after upgrading, since the existing generateSecretKeys task leaves an already-set value untouched.	9.8	More Details
CVE-2026-19256	The All In One Login WordPress plugin before 2.5.0 does not adequately restrict the number of attempts that can be made against the short numeric code used by its default-enabled passwordless email login, and does not feed those failed attempts into its own brute-force protection, allowing unauthenticated attackers to take over any account including administrators.	9.8	More Details
CVE-2026-69050	Out-of-bounds memory access in a device driver due to improper resource state tracking.	9.8	More Details
CVE-2026-68991	In the Samsung Exynos ENN NeuralNetworks HAL, improper input validation during request processing can cause memory corruption and lead to a denial of service condition.	9.8	More Details
CVE-2026-48174	In the NR RRC component, improper handling of messages before authentication triggers a data abort, which leads to a denial-of-service condition.	9.8	More Details
CVE-2026-113584	The placester WordPress plugin through 1.4.3 does not perform any capability, nonce or ownership check on an AJAX action that updates account details, allowing unauthenticated attackers to overwrite any user's email address, including an administrator's, and take over the account through the standard password-reset flow.	9.8	More Details
CVE-2026-33972	In the Exynos modem's IMS stack, Out of Bound access occurs due to improper validation.	9.8	More Details
CVE-2026-33971	In the LTE RRC component, improper handling of messages before authentication triggers a data abort, which leads to a denial-of-service condition.	9.8	More Details
CVE-2026-54384	VitaFit cloud API before 2026-10-30 contained an authentication bypass vulnerability that allows remote attackers to obtain a full session for a victim's account by submitting a linked Google or Facebook account identifier to the POST /front/login/sns/ endpoint without providing proof of ownership from the identity provider. Attackers can forge a login using an identifier exposed through account enumeration to read and modify the victim's profile and delete the account's authentication record, preventing the legitimate user from logging in.	9.8	More Details
CVE-2026-54143	OpenHuman is an open-source agent harness available as a desktop application and Rust library. Before version 0.57.13, an attacker who can send messages to a configured external channel can cause the agent to create persistent shell cron jobs without human approval. The scheduler later executes these jobs with the privileges of the OpenHuman runtime user. Command validation also permits leading environment assignments that can redirect allowed commands to executable helpers. The demonstrated exploit requires a suitable helper executable already present on the host. This can lead to unauthorized persistent command execution and compromise data and resources accessible to OpenHuman. This issue is fixed in version 0.57.13.	9.8	More Details

CVE-2026-102895	GPUStack is an open-source GPU cluster manager for AI model serving and GPU instance provisioning. Prior to 2.2.0, get_current_user in gpustack/api/auth.py treated a loopback request source as the built-in administrator when force_auth_localhost was false, which was the default. A remote request could appear to originate from 127.0.0.1 because client_ip_getter accepted a same-host reverse proxy peer or a client-supplied X-GPUStack-Real-IP loopback value. The bypass allowed unauthenticated administrative access, including user and model changes, persistent administrator API-key creation, disclosure of worker and cloud-provider secrets, and code execution through POST /v2/inference-backends/from-yaml. Exploitation was observed in the wild against a 2.1.1 deployment. This issue is fixed in version 2.2.0.	9.8	More Details
CVE-2026-82418	IBM Watson Speech Services Cartridge 4.0.0 through 5.4.0 could allow a remote attacker to execute arbitrary code due to a use-after-free vulnerability.	9.8	More Details
CVE-2025-71457	vtenext 25.02 before 25.02.1 contains an authentication bypass vulnerability that allows unauthenticated attackers to change any account password via hub/rpwd.php without token verification. Attackers knowing a valid user_name can send action=change_password to RecoverPwd::displayChangePwd() and log in as administrators lacking two-factor authentication.	9.8	More Details
CVE-2026-121953	FreeRDP before 3.32.2 has a use-after-free in the client's rdpgfx dynamic virtual channel: a duplicate-name channel with a new ChannelId overwrites the listener's single callback slot, which rdpgfx_on_close frees without clearing. A malicious RDP server can open and close such a channel, then send a PDU on the original channel to crash the client or potentially execute code.	9.8	More Details
CVE-2026-121952	FreeRDP before 3.32.2 has an out-of-bounds write in the proxy because rdp_read_bitmap_cache_v2_capability_set rejects only numCellCaches values above 5, yet the bitmap cache v2 cell array is later accessed at fixed indices 0 through 4. A client connecting to the proxy can declare fewer than five cell caches in its Confirm Active, causing heap corruption, heap data leakage to the backend, or a crash.	9.8	More Details
CVE-2026-39430	On HP Poly EagleEye Cube USB 1.3.1-001267 devices, the administrator authentication flow is broken: session management and access controls are not enforced device-side. Thus, an unauthenticated user can change administrator-level settings (without logging in) via a modified client that bypasses the login step or via a custom client to make the underlying administrator API calls. This allows unauthenticated users to perform administrative actions too such as exporting configuration files that include the internal device credentials for the administrator user and other network systems.	9.8	More Details
CVE-2026-122006	The activestorage gem before 8.1.4.1 for Ruby on Rails, when ImageMagick attachment processing occurs, can allow server read and write operations (e.g., reading secret_key_base) because the ImageMagick analyzer runs when a file is attached, and there is not an ImageMagick security policy to block unintended functionality.	9.8	More Details
CVE-2026-65555	Incorrect Privilege Assignment vulnerability in Uncanny Owl Uncanny Toolkit for LearnDash uncanny-learndash-toolkit allows Privilege Escalation.This issue affects Uncanny Toolkit for LearnDash: from n/a through 3.8.2.	9.8	More Details
CVE-2026-119481	Incorrect Privilege Assignment vulnerability in Crocoblock JetFormBuilder jetformbuilder allows Privilege Escalation.This issue affects JetFormBuilder: from n/a through 3.6.7.1.	9.8	More Details
CVE-2026-120647	CGI versions before 5.00 for Perl allow Content-Disposition parameter injection via unescaped double quotes in the header attachment filename. header(-attachment => $name) writes $name into the quoted filename parameter of Content-Disposition without escaping double quotes. An application that passes request data as the attachment name can be made to send a second filename parameter, changing the name the response is saved under.	9.8	More Details
CVE-2026-81815	SQL Injection in the entity engine's generic performFind service in Apache OFBiz 24.09 before 24.09.08 on MySQL/MariaDB-backed deployments allows a remote unauthenticated attacker to disclose arbitrary rows from the queried entity by submitting an ignore-case find request (e.g. _ic=Y) with a crafted value, causing SqlJdbcUtil.addValueSingle to inline the EntityFunction-wrapped value directly into the SQL text using ANSI-only single-quote doubling instead of binding it as a parameter, which is insufficient on MySQL/MariaDB because those dialects also honor backslash escapes, letting a backslash-terminated payload break out of the string literal and turn the WHERE clause into a tautology. The default Derby datasource and PostgreSQL are not affected because they do not interpret backslash as an escape character in this context. Users are recommended to upgrade to version 24.09.08, which fixes this issue.	9.8	More Details
CVE-2026-48173	In the NAS message handler, improper validation of the length field in NAS message causes memory corruption	9.8	More Details
CVE-2026-123198	LMFDB before commit 01829bd contains a server-side template injection vulnerability in the render_knowl function that allows unauthenticated attackers to inject Jinja expressions via request parameters. Attackers can supply crafted query-string values or 'content' data to /knowledge/render/<ID> to reach Python builtins and execute operating system commands as the web application account.	9.8	More Details
CVE-2026-119757	BTCPay Server before 2.4.2, including 2.4.2 release candidates, contains an information disclosure vulnerability that allows unauthenticated remote attackers to retrieve .macaroon credential files for an LND (Lightning Network Daemon) node. Attackers can use the exposed macaroon to gain full control of the LND node, including moving funds, resulting in theft of funds from affected deployments.	9.8	More Details

CVE-2026-116779	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to 1.11.3, sofia_presence_handle_sip_i_message() split the To user of an inbound SIP MESSAGE on a plus sign and treated the left side as a chat protocol selector. Selecting the api chat proto reached switch_api_execute(), allowing a peer whose MESSAGE was accepted to run FreeSWITCH API commands, including operating-system command sinks, with the daemon's privileges. Inbound chat is enabled on the stock internal and external profiles, and any authenticated profile account is sufficient; stock directory users without password material can also remove that barrier in affected configurations. The flaw permits configuration and credential disclosure, arbitrary call control, and command execution, and exploitation has been observed in the wild. This issue is fixed in version 1.11.3.	9.8	More Details
CVE-2026-110955	The Wurdey WordPress plugin through 1.0.0 does not verify a request signature before logging a user in, allowing unauthenticated attackers to authenticate as an administrator knowing only the administrator's username.	9.8	More Details
CVE-2026-123294	In JetBrains Hub before 2026.2.52556 privilege escalation was possible by changing email authentication details during the verification flow	9.6	More Details
CVE-2026-123831	In JetBrains CLion before 2026.2, 2026.1.4 code execution was possible in Safe Mode via Meson project settings	9.6	More Details
CVE-2026-17353	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information and bypass security restrictions due to server-side request forgery.	9.6	More Details
CVE-2026-17396	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to SQL injection.	9.6	More Details
CVE-2026-54378	VitaFit cloud API before 2026-10-30 contained a broken access control vulnerability that allows any authenticated user to obtain temporary AWS credentials by calling the POST /front/user/s3/token/ endpoint. Attackers can use these improperly scoped credentials to list the shared storage bucket and read or overwrite other users' stored files, enabling unauthorized cross-user data access and manipulation.	9.6	More Details
CVE-2026-115770	Pocket ID is an OIDC provider that allows users to authenticate with their passkeys to services. From 2.2.0 until 2.12.0, SendEmailVerification uses the token model in backend/internal/model/email_verification_token.go to bind an email-verification token only to the user's identifier, while UpdateUser can change the account email without invalidating the outstanding token and VerifyEmail marks the current address as verified. An ordinary user can request a token for an address they control, change the account to an arbitrary unused address, and redeem the old token so Pocket ID publishes the new address with email_verified set to true. The default affected configuration uses emailsVerified=false and allowOwnAccountEdit=true; the target address must not already belong to another Pocket ID user. A relying application that trusts a verified email for automatic account matching or provisioning can link the attacker's identity to another user's account, while applications that rely exclusively on the stable OIDC sub claim are not affected by that downstream consequence. This issue is fixed in version 2.12.0.	9.6	More Details
CVE-2026-17299	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to perform arbitrary file reads and server-side request forgery due to unrestricted resolution of external references. Externally referenced content in submitted definitions is not sufficiently restricted when processed, and the retrieved content could be returned to the attacker.	9.6	More Details
CVE-2026-17297	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote attacker to perform an account takeover due to an open redirect vulnerability. The redirect address used during sign-in is not sufficiently validated, which could allow authentication results to be sent to an attacker-controlled location.	9.6	More Details
CVE-2026-17296	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to server-side request forgery.	9.6	More Details
CVE-2026-18535	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 are vulnerable to a Regular Expression Denial of Service (ReDoS) attack and to improper neutralisation of wildcard query operators.	9.6	More Details
CVE-2026-77596	Kubeflow Pipelines enables users to build and deploy portable, scalable machine learning workflows. Prior to 2.18.0, the multi-user HTTP endpoints POST /apis/v2beta1/pipelines/upload and POST /apis/v2beta1/pipelines/upload_version call canUploadVersionedPipeline, which returns without SubjectAccessReview when the target namespace is empty while REQUIRE_NAMESPACE_FOR_PIPELINES defaults to false. A low-privilege tenant can create shared pipelines or inject attacker-controlled versions into existing shared pipelines without the required write permission; if the API server is directly reachable without an authenticating proxy, an unauthenticated caller can exploit the same bypass, while deployments protected by such a proxy do not expose anonymous access. An enabled unpinned recurring run that follows the latest version can then execute the injected specification in another tenant's namespace under that workload's service account, while pinned or embedded-specification runs are not automatically substituted. This issue is fixed in version 2.18.0.	9.6	More Details
	The Tournamatch WordPress plugin before 4.7.1 does not validate or restrict the path of a previously stored		

CVE-2026-121379	profile or team image before deleting it when a new image is uploaded, allowing users with a role as low as Subscriber to delete arbitrary files on the server, such as wp-config.php, which can lead to a full site takeover.	9.6	More Details
CVE-2026-17394	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to improperly controlled modification of object attributes. A user-supplied value could change an access-related setting that should be controlled by the system, which could expose sensitive information.	9.6	More Details
CVE-2026-86044	JupyterLab Desktop is the cross-platform desktop application for JupyterLab. Prior to 4.6.2-1, JupyterLab Desktop exposed getServerInfo to the renderer without confirming that the current page still had the local Jupyter server origin. In a local managed session using JupyterLab before 4.4.8, an attacker can place a crafted MathJax link in an untrusted notebook. If a victim opens the notebook and clicks the link, the existing renderer navigates to an attacker-controlled site while retaining access to the preload bridge. The site can call getServerInfo to obtain the local server URL and authentication token, then use the Jupyter REST API to create and trust a notebook that executes arbitrary code as the victim. Users whose environment already uses JupyterLab 4.4.8 or later are unaffected because the corrected link handling breaks the first step of the chain. This vulnerability is fixed in 4.6.2-1.	9.6	More Details
CVE-2026-123832	In JetBrains CLion before 2026.2 code execution was possible in Safe Mode via JSON compilation database	9.6	More Details
CVE-2026-102940	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to 8.4.0, controllers/C_Document.class.php write actions, including move_action_process(), do not verify the caller's access to the source document, current patient and category, or destination patient and category before Document::change_patient() performs the mutation. A low-privilege authenticated user can reassign an arbitrary document to a patient or category the user can access and then retrieve it through the normally protected read path. The reassignment occurs before a later list rendering check, so a final HTTP 403 response does not mean the unauthorized write was blocked. This issue is fixed in version 8.4.0.	9.6	More Details
CVE-2026-18838	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote attacker to obtain sensitive information and modify API configurations due to improper authentication. Identity information supplied in requests is not sufficiently verified, which could allow a caller to impersonate another user.	9.4	More Details
CVE-2026-17409	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote attacker to execute unauthorized administrative operations and obtain sensitive information due to improper handling of case sensitivity. Access controls are not applied consistently to all variations of a request, which could allow restricted operations to be reached.	9.4	More Details
CVE-2026-17344	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote attacker to obtain sensitive information due to server-side request forgery. A service that can be reached without authentication could be made to send requests to unintended destinations.	9.3	More Details
CVE-2026-57566	Readest is a modern, feature-rich ebook reader designed for seamless cross-platform access and an intuitive reading experience. Prior to 0.11.10, the unauthenticated /api/opds/proxy route in apps/readest-app/src/app/api/opds/proxy/route.ts accepted an attacker-controlled URL and fetched it server-side without restricting the scheme, blocking private, loopback, link-local, or metadata hosts, or revalidating destinations during automatic redirect following. The route also accepted caller-controlled outbound headers and Authorization values and reflected the upstream status and response body. A remote attacker could use the service as an open request proxy and, on Node, Docker, or other self-hosted deployments with internal-network access, retrieve cloud metadata or internal-service responses. Cloudflare Workers deployments restrict access to link-local and private destinations, which reduces the internal-network impact there, but the unauthenticated public fetch-and-reflect behavior remains. This issue is fixed in version 0.11.10.	9.3	More Details
CVE-2026-17329	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote attacker to obtain sensitive information due to improper validation of endpoint URLs.	9.3	More Details
CVE-2026-100144	The IVPAY payments WordPress plugin through 1.0.8 does not sanitise a value from its payment callback before using it in a SQL statement, and treats an empty API key, which is its own default, as valid authentication, allowing unauthenticated attackers to read arbitrary data from the database.	9.3	More Details
CVE-2026-17131	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote attacker to obtain sensitive information due to server-side request forgery. Restrictions on outbound requests can be bypassed, so the server could be made to contact unintended destinations and return the response.	9.3	More Details
CVE-2026-48705	MONAI (Medical Open Network for AI) is an AI toolkit for health care imaging. Prior to 1.6.1, PydicomReader._get_affine() trusts non-finite values in the DICOM PixelSpacing, ImagePositionPatient, and ImageOrientationPatient fields and composes them into an affine matrix without validation. An unauthenticated attacker who can upload a crafted DICOM to a default MONAILabel deployment can propagate NaN or infinity values through LoadImaged, Spacingd, model inference, and output writing, causing inference failures, persistent datastore poisoning, or geometrically corrupted results. This issue is fixed in version 1.6.1.	9.3	More Details

CVE-2026-16918	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote attacker to access internal network resources due to server-side request forgery.	9.3	More Details
CVE-2026-18836	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote attacker to obtain sensitive information due to server-side request forgery. The affected component can be made to send requests to unintended destinations and return the response to the attacker.	9.3	More Details
CVE-2026-113780	ESF-IDF is the Espressif Internet of Things (IOT) Development Framework. From 5.5.5 until 5.5.6, 6.0.4, and 6.1.1, the esp_tee trap entry in esp_tee_vectors_plic.S and esp_tee_vectors_clic.S saves a caller-controlled register frame through the REE-supplied stack pointer before switching to the trusted TEE stack or validating the pointer. A local unprivileged REE application can direct this machine-mode write into TEE-exclusive memory on ESP32-C5, ESP32-C6, ESP32-C61, and ESP32-H2 devices, breaking the REE/TEE isolation boundary and potentially corrupting TEE control-flow data for code execution, denial of service, or system crashes. Both secure-service ecall and interrupt entry paths contain the vulnerable ordering. This issue is fixed in version 5.5.6 and is scheduled to be fixed in versions 6.0.4 and 6.1.1.	9.3	More Details
CVE-2026-121802	@better-auth/expo before 1.7.16 allows certain account-takeover outcomes (e.g., unauthenticated changes of any account's email address), because it signs a caller-supplied state value without checking whether that value had been issued by the server. NOTE: the application secret must be rotated after updating to a fixed version.	9.1	More Details
CVE-2026-120642	CGI versions before 5.00 for Perl return request-derived values untainted under taint mode. The upload filename, uploadInfo values, some path_info and script_name values, Accept results, and the name lists from url_param and cookie are returned without the taint flag, as is a cookie named expires from 4.67 on. These values come from regex captures or hash keys, which Perl does not taint, so they pass -T checks unvalidated.	9.1	More Details
CVE-2026-123959	A security flaw has been discovered in TOTOLINK CA300-PoE 6.2c.884. The impacted element is the function setLanguageCfg of the file /cgi-bin/cstecgi.cgi. Performing a manipulation of the argument langType results in buffer overflow. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks.	9.1	More Details
CVE-2026-83493	A flaw was found in distributed-workloads. A remote attacker could exploit a vulnerability in the pull_request_target workflow by submitting a specially crafted pull request. This workflow processes untrusted code from the pull request author while operating with the base repository's sensitive secrets, such as the SNYK_TOKEN, and its default write token. Consequently, an attacker could exfiltrate these secrets, leading to unauthorized access to the Snyk integration and potential control over the repository.	9.1	More Details
CVE-2026-120644	CGI::Cookie versions before 5.00 for Perl allow cookie attribute injection via unvalidated path, domain and expires values. The path, domain and expires values are written into the Set-Cookie header without checking for semicolons or control characters. An application that sets them from request data can be made to add other cookie attributes, such as Domain or SameSite.	9.1	More Details
CVE-2026-121930	A weakness has been identified in Linksys WRT54GL 4.30.18. The affected element is the function system of the file apply.cgi of the component Ping Diagnostic. This manipulation of the argument ping_ip causes os command injection. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way. This vulnerability only affects products that are no longer supported by the maintainer.	9.1	More Details
CVE-2026-121931	A security vulnerability has been detected in Linksys WRT54GL 4.30.18. The impacted element is the function system of the file apply.cgi of the component Traceroute Diagnostic Function. Such manipulation of the argument traceroute_ip leads to os command injection. The attack can be launched remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way. This vulnerability only affects products that are no longer supported by the maintainer.	9.1	More Details
CVE-2026-122041	The Checkout Field Editor for WooCommerce (Pro) plugin for WordPress is vulnerable to unauthorized deletion of arbitrary attachments due to a missing capability/ownership check in the ajax_remove_uploaded() function in versions up to, and including, 3.8.0. The handler is registered for both wp_ajax and wp_ajax_nopriv and is gated solely by the 'file_handling_nonce' nonce, which is emitted inside the public checkout page markup (data-nonce attribute) whenever a File Upload checkout field is configured. This makes it possible for unauthenticated attackers to delete arbitrary attachments (including those belonging to other users or posts) by submitting a crafted attachment_id, which can lead to loss of important media and potential denial of service.	9.1	More Details
CVE-2026-120984	A flaw was found in the Keycloak server's client management component. When a client is created or imported with authorization services enabled, the system fails to properly clear an internal session attribute used during the setup process. This allows an authenticated attacker with client management permissions to bypass security controls and upload a malicious JavaScript policy, which is then executed on the server when an authorization request is made. Successful exploitation could allow the attacker to run arbitrary code on the server, potentially compromising the entire system.	9.1	More Details
	The Appointment Booking Plugin – LatePoint | Calendar & Scheduling for WordPress plugin for WordPress is vulnerable to Authentication Bypass via Account Takeover in all versions up to, and including, 5.7.6. This is		

CVE-2026-118066	due to the `OsModel::build_conditions_query()` function in `lib/models/model.php` comparing WHERE-clause values against the literal strings `''IS NULL''` and `''IS NOT NULL''` and concatenating a match directly into SQL without binding it as a parameter, a flaw that neither `sanitize_text_field()` nor the 5.7.5 `is_scalar()` hardening guard closes, since both pass the scalar sentinel through unchanged. This makes it possible for unauthenticated attackers to send `params[password_reset_token]=IS NOT NULL` to the public `customer_cabinet__change_password` AJAX route to match every non-null `account_nonse` value, resolving to the lowest-id customer and overwriting that customer's password to an attacker-chosen value — granting full access to their bookings, orders, and PII, and, when the `wp_users_as_customers` option is enabled, takeover of the linked WordPress subscriber or customer-role account. The attacker can first identify the target customer's email by sending `params[order_intent_key]=IS NOT NULL` to the public `steps__start_from_order_intent` route, which returns the name and email from the first matching order intent, and can then self-arm the required 15-minute password-reset freshness window by triggering a reset for that customer directly.	9.1	More Details
CVE-2026-88800	The MDJM Event Management and Mobile Events Manager WordPress plugins through 1.7.8.7 act on a role deletion request on every page load with no capability check and no nonce, and the guard meant to protect roles that have users assigned reads a different part of the request from the one that selects what is deleted, allowing unauthenticated attackers to remove any WordPress role including administrator, which permanently strips every user of their capabilities.	9.1	More Details
CVE-2026-17338	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to broken object-level authorization.	9.1	More Details
CVE-2026-114630	The ELEX WordPress HelpDesk & Customer Ticketing System plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the factory_reset function in all versions up to, and including, 3.3.8 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). This vulnerability is exploitable via a two-step chain: an unauthenticated attacker first stores an arbitrary ticket_attachment_path value by submitting a ticket through the nopriv eh_crm_new_ticket_post AJAX endpoint (whose nonce is publicly exposed via the [wsdesk_support] shortcode), then triggers the factory_reset routine via a GET request to wp-admin/admin.php?page=wsdesk_factory_reset, which is guarded only by is_admin() — a request-type check — rather than a capability check, causing unlink() to be called on the attacker-supplied path.	9.1	More Details
CVE-2026-112902	Pillow is a Python imaging library. In versions through 12.3.0, the libtiff TIFF encoder can pass arguments to TIFFSetField() that do not match libtiff's definition of the corresponding tag. When an application saves attacker-controlled image metadata through this encoder, crafted tag values can cause invalid memory reads, copying process memory into the encoded output or crashing the process. Applications that return the encoded output to an attacker can disclose that memory. The issue is reachable when re-saving compressed TIFF images and through certain conversions that preserve EXIF metadata into compressed TIFF output. This vulnerability is fixed in version 13.0.0.	9.1	More Details
CVE-2026-69068	Insufficient length validation in the GNSS firmware loader may lead to corruption of kernel memory.	9.1	More Details
CVE-2026-116785	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to 1.11.2, ws_read_frame() decoded a WebSocket frame's 64-bit extended payload length with a 32-bit byte swap and narrowed the result into a signed length. A value whose surviving low word became negative bypassed the signed size check and was reinterpreted as an enormous unsigned count, causing client bytes to overwrite memory beyond the 64 KiB receive buffer. Any client completing a /socket WebSocket upgrade on an enabled mod_xml_rpc endpoint reached the parser before HTTP authentication; both the module and WebSocket endpoint are disabled by default. The heap overwrite can corrupt connection pointers and crash FreeSWITCH, ending every concurrent session, although remote code execution has not been demonstrated. This issue is fixed in version 1.11.2.	9.1	More Details
CVE-2026-69006	Insufficient validation of length fields in the GNSS firmware loader can result in kernel-memory corruption.	9.1	More Details
CVE-2026-48186	Improper handling of messages before AS security activation can cause unexpected behavior	9.1	More Details
CVE-2026-117691	A flaw was found in the SAML HTTP-Redirect binding implementation of Keycloak. The issue occurs because the server processes percent-encoded parameter names (like %53AMLResponse) while the signature verification logic only checks literal parameter names. An attacker can use this discrepancy to provide a crafted, unsigned SAML message that the server processes instead of a legitimately signed one, leading to full account takeover of federated users.	9.1	More Details
CVE-2026-68935	Chartbrew is an open-source web application for creating charts from databases and APIs. In versions 4.8.5 through 5.2.2, API connection creation and update operations accept the internal allowPrivateHost field from user input. An authenticated user with permission to manage API connections can enable this field to bypass private and reserved-network destination restrictions. An upgrade migration also enables the override on pre-existing API connections. The per-connection setting takes precedence over CB_ALLOW_PRIVATE_NETWORK_CALLS , so disabling that instance option does not protect connections with	9.1	More Details

	the override enabled. Successful exploitation allows requests to internal HTTP services reachable from the Chartbrew server, potentially disclosing information or triggering unauthorized actions depending on the target service. Recognized cloud metadata endpoints remain separately blocked. This issue is fixed in version 5.2.3.		
CVE-2026-48183	Improper permission handling during buffer operations allows untrusted applications to create memory mappings with inappropriate permissions	9.1	More Details
CVE-2026-116790	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to 1.11.2, FreeSWITCH's inbound ICE handling accepted every connectivity check without cryptographically validating its STUN MESSAGE-INTEGRITY attribute. A network peer able to reach an ICE-enabled leg's media port could forge an ICE connectivity check without SDP credentials, nominate its own address, redirect RTP and DTLS traffic, and terminate the legitimate media path. On unencrypted legs this enables eavesdropping and media injection, while all WebRTC and SIP legs that negotiate ICE are in scope. Version 1.11.2 introduces the remediation, which requires ice_verify_message_integrity=true.	9.1	More Details
CVE-2026-46350	dcmjs is a JavaScript implementation of DICOM manipulation. Prior to 0.52.0, the DecimalString and IntegerString implementations in src/ValueRepresentation.js sanitize text with a permissive regular expression and pass the result to JavaScript's Number constructor without validating finiteness or the DICOM value-representation rules. Scientific notation overflow in a DS or IS field can produce positive or negative Infinity, while stripping alphabetic characters from signed infinity text can leave a sign-only string that converts to NaN. IntegerString also accepts exponent notation and values outside the DICOM signed 32-bit IS range. Applications that trust these parsed values can propagate invalid numbers into spatial geometry, display windowing, dose scaling, frame counts, rescaling, or volume reconstruction, causing incorrect calculations or disrupted processing. This issue is fixed in version 0.52.0.	9.1	More Details
CVE-2026-69043	In the Samsung Exynos GPU driver, improper synchronization during buffer object creation and closing can lead to memory corruption	9.1	More Details
CVE-2026-122321	Kyverno 1.18.0 before 1.19.2 contains a signature verification bypass in verifyImages because cached verification results are keyed by the image reference string (such as a tag) rather than bound to the verified digest, so cache hits skip signature and attestation checks. An attacker who can submit workloads and move a registry tag can warm the cache with a signed image, repoint the tag, and have Kyverno admit the workload and use mutateDigest to pin the unverified digest.	9.1	More Details
CVE-2026-17292	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to take over ownership of other organizations due to broken object-level authorization. Access checks on organization objects are incomplete, which could allow ownership of organizations the user does not control to be changed.	9.1	More Details
CVE-2026-76171	In Apache James server prior version 3.9.1 improper validation in JMAP webPush SSRF validation did lead to the possibility to reach internal addresses. Users are recommended to upgrade to version 3.9.1 which fixes this issue.	9.1	More Details
CVE-2026-74841	In multitenant deployments, ContextFilter and LoginWorker built a per-tenant delegator name from a request-supplied userTenantId parameter and requested a delegator for it before confirming the tenant existed. DelegatorFactory's internal cache retains every delegator name it is asked to resolve, including ones that fail to resolve, so an unauthenticated attacker could submit a stream of arbitrary tenant IDs to grow this cache without bound, driving unnecessary memory and database load.	9.1	More Details
CVE-2026-100358	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to 7.15.2 and 8.10.2, the Studio Dropdown Editor passes $dropdown_name through html_entity_decode() and writes the result verbatim into a PHP language file under custom/ that is included on later page loads. An administrator can inject persistent PHP that executes as the web-server account, survives cache clears, and compromises application and host confidentiality, integrity, and availability. This issue is fixed in versions 7.15.2 and 8.10.2.	9.1	More Details
CVE-2026-17339	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to access or delete resources belonging to other tenants due to path traversal.	9.1	More Details
CVE-2026-74756	Some docker-compose shipped by the project exposes by default Webadmin REST API publically without proper authentication setup. Version 3.9.1 onward sets a random credential by default on unprotected webadmin endpoints to prevent this while retain convenience.	9.1	More Details
CVE-2026-102894	GPUStack is an open-source GPU cluster manager for AI model serving and GPU instance provisioning. From 0.7.1 until 2.2.2, the /auth/saml/callback endpoint decoded SAML XML, used its NameID and attributes to resolve or provision a user, and minted a gpustack_session JWT without calling OneLogin_Saml2_Auth.process_response to verify the signature, issuer, audience, destination, or time conditions. Any network client could submit an identity for an existing user, including an administrator, or provision a new non-administrator account, even when SAML was not configured. Response and Assertion identifiers were not consumed, so captured signed responses could also be replayed. This issue is fixed in version 2.2.2.	9.1	More Details
CVE-2026-	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive		

17066	information and modify or delete data belonging to other tenants due to missing authorization.	9.1	More Details
CVE-2026-121491	The Fiber Admin WordPress plugin before 4.0.1 does not validate or escape a request header before writing it into a PHP file it regenerates on an unprotected admin hook, allowing unauthenticated attackers to execute arbitrary code when its custom database error page is enabled and they win a race against an administrator saving its settings.	9.0	More Details
CVE-2026-63774	Insufficient input validation in the PowerSYSTEM Center report designer allows an authenticated user to execute unauthorized SQL commands.	9.0	More Details
CVE-2026-63017	Incorrect authorization in PowerSYSTEM Center allows a low-privileged, authenticated user to access resources normally limited to administrators.	9.0	More Details
CVE-2026-123279	In JetBrains Datalore before 2026.4 code execution was possible in a notebook's computation by view-only collaborators	9.0	More Details
CVE-2026-122120	In Yealink Plug-in Softwares before 2.35.219.0, there is an unauthorized file write vulnerability under specific scenarios, which may be exploited by attackers to achieve remote code execution.	9.0	More Details
CVE-2026-17403	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote attacker to gain full administrative control due to the use of hard-coded credentials.	9.0	More Details
CVE-2026-54141	OpenHuman is an open-source agent harness available as a desktop application and Rust library. Before 0.57.13, a remote direct message received through a configured Yuanbao channel is converted into a generic channel AgentTurnRequest that uses the default tool policy without establishing an interactive approval context. Under the default Supervised autonomy policy with Node enabled, node_exec is classified as a write operation that should prompt for approval, but ApprovalGate treats missing APPROVAL_CHAT_CONTEXT as a non-interactive turn and allows execution. Because Yuanbao direct messages are open by default, an external sender who can message the connected bot can influence the agent to execute JavaScript and operating-system commands as the OpenHuman user without an approval prompt. The issue requires a configured Yuanbao channel, the default approval-requiring policy state, Node availability, and successful model selection of node_exec. This issue is fixed in version 0.57.13.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2026-17280	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote attacker to perform unauthenticated brute-force attacks to obtain valid credentials due to improper restriction of excessive authentication attempts.	8.9	More Details
CVE-2026-97377	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to 7.15.2 and 8.10.2, the legacy SOAP portal method portal_get_entry_list propagates caller-controlled where and order_by values into SQL query construction without sufficient neutralization. A low-privileged portal API user can perform blind SQL injection to disclose database metadata and sensitive records, affect query behavior, and consume resources. This issue is fixed in versions 7.15.2 and 8.10.2.	8.8	More Details
CVE-2026-121866	The iLeads SMS Gateway by Exsile WordPress plugin before 2.0.0 does not check capabilities or nonces in several AJAX actions that update a site option chosen by the request, allowing any authenticated user, such as a subscriber, to change arbitrary WordPress options and escalate to administrator, for example by enabling registration with administrator as the default role.	8.8	More Details
CVE-2026-121848	The Magic Link WordPress plugin before 2.2.6 does not check that the user requesting a login link is authorised to generate one for the chosen account, allowing any authenticated user, such as a subscriber, to generate a working login link for an administrator and log in as them.	8.8	More Details
CVE-2026-17405	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to broken object-level authorization. Access checks on keystore objects do not confirm that the requesting user is permitted to read them, which could expose keystore information.	8.8	More Details
CVE-2020-9709	Adobe Photoshop versions Photoshop CC 2019, and Photoshop 2020 have a security bypass vulnerability. Successful exploitation could lead to privilege escalation.	8.8	More Details
CVE-2026-121816	Herowatch Mini developed by About Time Technologies has a Missing Authentication vulnerability. Unauthenticated remote attackers can connect to the affected device's ADB service and obtain an ADB shell, thereby accessing device resources or performing related operations.	8.8	More Details
CVE-2026-17335	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to execute arbitrary code due to path traversal. File paths in uploaded content are not sufficiently validated, which could allow files to be written outside the intended location and code to be executed.	8.8	More Details

CVE-2026-77690	ZohoCorp ManageEngine Key Manager Plus versions before 7151 were vulnerable to a Command Injection vulnerability that allowed authenticated users with certificate deployment privileges to execute arbitrary commands through specially crafted input when configuring a deployment target.	8.8	More Details
CVE-2026-16511	Two RTIO syscall verifiers, in subsys/rtio/rtio_syscalls.c (subsys/rtio/rtio_handlers.c before v4.3.0), did not validate user-supplied pointers before the kernel wrote through them. z_vrfy_rtio_sqe_cancel() performed no validation at all. It passed the caller's struct rtio_sqe pointer straight to z_impl_rtio_sqe_cancel(), which converts it with CONTAINER_OF to a struct rtio_iodev_sqe, ORs RTIO_SQE_CANCELED (BIT(3)) into its 16-bit flags field in supervisor mode, then loads its next pointer and repeats until that pointer is NULL. The syscall takes no RTIO context argument, so it needs no object grant: any user-mode thread on a CONFIG_USERSPACE build can set that bit in a 16-bit word at an address of its choosing in kernel memory, and the kernel continues the write along whatever pointer chain it finds at the corresponding offset. Setting chosen bits in kernel data structures, such as object permission or thread state fields, can be used to escalate privilege from user mode. z_vrfy_rtio_sqe_copy_in_get_handles() validated its RTIO context and the input SQE array, but only NULL-checked the handle out-parameter before writing a kernel SQE pointer through it, with no K_SYSCALL_MEMORY_WRITE check. A user thread that holds a granted RTIO context can therefore make the kernel store a pointer value at an arbitrary address. The fixes validate the handle out-parameter as writable, bound the cancel handle to real submission-pool storage, and require permission on the RTIO context that owns the matching pool. Without that last check a bounded handle still let any user thread cancel submissions belonging to other contexts, silently aborting their I/O. Systems built without CONFIG_USERSPACE or without CONFIG_RTIO are unaffected.	8.8	More Details
CVE-2026-121940	Stonewuu ai-fusion-video before 1.3.0 contains an insecure direct object reference vulnerability that allows authenticated users to access other users' projects by supplying unscoped object ids. Attackers can enumerate auto-increment ids on /api/project, /api/asset and /api/script handlers to read, overwrite, cascade-delete data, and add themselves as project members.	8.8	More Details
CVE-2026-16716	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to bypass security restrictions to access and modify sensitive information due to improper restriction of security token assignment.	8.8	More Details
CVE-2026-121994	A stack buffer overflow in the GDB client's remote protocol handler allows an attacker-controlled debug target to execute arbitrary code in the GDB process. The vulnerability exists in fetch_register_using_p, which decodes a stub's register reply into an alloca-sized buffer without bounding writes by the register width.	8.8	More Details
CVE-2026-54145	OpenHuman is an open-source agent harness available as a desktop application and Rust library. In affected versions before 0.57.5, the approval gate uses the JSON-RPC bearer token as an approval session identifier. This exposes the credential through persisted approval records, events, debug logs, and RPC responses, including during normal desktop operation. An attacker who obtains these artifacts can recover the token and access the core RPC interface while it remains valid. This can expose sensitive agent and integration data and permit privileged operations. Stable tokens remain usable until rotated; launch-specific tokens remain usable while the corresponding core instance is active. The fix is included in version 0.57.5.	8.8	More Details
CVE-2026-54146	OpenHuman is an open-source agent harness available as a desktop application and Rust library. From 0.53.15 before 0.57.5 on macOS, core_process.rs in the Tauri desktop process publishes the per-launch OPENHUMAN_CORE_TOKEN bearer credential in its process environment even though the core now runs as an in-process task. Another process running as the same user can read that environment through the macOS KERN_PROCARGS2 process-inspection interface, recover the token together with the local host and port, and authenticate to the core JSON-RPC service with the authority of the desktop frontend. The attacker can read agent memory and integrated-account data, invoke privileged actions, change configuration, and stop or disrupt services without root access, developer mode, or changes to System Integrity Protection. This issue affects Intel and Apple Silicon macOS systems. This issue is fixed in version 0.57.5.	8.8	More Details
CVE-2026-82413	ntopng is a web-based network traffic monitoring application. Prior to 6.7.260717, scripts/lua/rest/v2/add/host/to_scan.lua and scripts/lua/rest/v2/exec/host/schedule_vulnerability_scan.lua accept scan_ports from any authenticated session, including non-administrator users, while deployments with login disabled expose the same request without authentication. The endpoints validate scan_ports with validateSingleWord, which permits shell metacharacters, and persist the value for the minute vulnerability-scan scheduler. The scheduler concatenates the value into an nmap command through nmap_scan_host and executes it through ntop.execCmd or ntop.execCmdAsync using popen. For the tcp_portscan and cve modules, a preliminary nmap -sn probe must first report the target as up before the attacker-controlled ports are used. When nmap is installed, this command injection allows arbitrary operating-system commands to execute as the ntopng service account without further user interaction. This issue is fixed in version 6.7.260717.	8.8	More Details
CVE-2026-77439	Immich is a self-hosted photo and video management solution. Prior to 3.0.3, an authenticated user with editor access to a shared album can change the existing owner's role because album member role updates do not protect the owner from modification. By demoting the owner and then promoting themselves, an editor can take ownership of the album, remove the original owner, and delete the album. This vulnerability is fixed in version 3.0.3.	8.8	More Details
CVE-2026-97175	A flaw was found in the idp-auto-link authenticator of the keycloak-services component, which handles user identity federation. The issue occurs when Keycloak automatically links an incoming identity from an external provider to an existing local account based on an email address without verifying if the provider has validated that email. This can allow an attacker to take over a victim's account by using a matching unverified email address at a brokered provider.	8.8	More Details

CVE-2026-100363	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to 7.15.2 and 8.10.2, the V8 module API exposes CRUD operations for administrator-only modules to any authenticated OAuth2 user. The affected flow begins at /Api/V8/module and uses ACLRoles, ACLActions, and Administration to carry attacker-controlled data or authorization state into the security-sensitive operation. A low-privileged user can create roles, change ACL levels, bind elevated roles, and alter global configuration to obtain administrator-equivalent control of CRM data and behavior. This issue is fixed in versions 7.15.2 and 8.10.2.	8.8	More Details
CVE-2026-100365	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to 7.15.2 and 8.10.2, AOR report generation concatenates an attacker-controlled stored field label into an ORDER BY clause without an allowlist. The affected flow begins at AOR_Reports and uses aor_fields, ORDER BY, and field label to carry attacker-controlled data or authorization state into the security-sensitive operation. An authenticated user with AOR Reports access can perform time-based extraction of password hashes and arbitrary table data and can hold database connections with expensive expressions. This issue is fixed in versions 7.15.2 and 8.10.2.	8.8	More Details
CVE-2026-123208	noname Electron desktop build v1.11.2 through v1.11.6.1 contains an unauthenticated local file server with wildcard CORS that allows malicious websites to read, overwrite, or delete installation files. Attackers can send cross-origin requests to /writeFile on localhost port 8089 to overwrite renderer scripts, executing JavaScript with Node.js access as the local user.	8.8	More Details
CVE-2026-63214	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to 7.15.2 and 8.10.2, legacy REST methods append an authenticated caller's query parameter as a SQL WHERE clause after insufficient structural validation. The affected flow begins at /service/v4_1/rest.php and uses get_entry_list, get_entries_count, and query to carry attacker-controlled data or authorization state into the security-sensitive operation. An account with list permission on a module can bypass the user_hash filter, retrieve password hashes and other database data, and use recovered administrative credentials to compromise the application. This issue is fixed in versions 7.15.2 and 8.10.2.	8.8	More Details
CVE-2026-69142	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to 7.15.2 and 8.10.2, the jjwg_Maps map marker endpoint uses the authenticated caller's distance value in the map_markers action without strict numeric validation or parameterization. An authenticated attacker can alter the SQL query, extract database data, modify query results, and consume resources. This issue is fixed in versions 7.15.2 and 8.10.2.	8.8	More Details
CVE-2026-122001	The Komfortkasse for WooCommerce WordPress plugin before 1.4.9 does not properly validate the authenticity of REST API requests, overriding WordPress's own nonce verification so that a request forged in a logged-in administrator's browser is accepted, which can be used to create a new administrator account and fully take over the site.	8.8	More Details
CVE-2026-87112	The QA Assistants – Driven by data plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 5.3.0 via the 'dlevent_ver' parameter. This is due to unrestricted PHP deserialization via wrap_unserialize_static() calling unserialize() without an allowed_classes restriction, combined with serialize_escape() failing to sanitize path traversal sequences in the raw_name parameter. This makes it possible for unauthenticated attackers to inject a PHP Object. The Guzzle FileCookieJar gadget present in the plugin's bundled Composer dependencies can be leveraged to perform an Arbitrary File Write, writing attacker-controlled content to an attacker-chosen filename, which can result in Remote Code Execution. Exploitation requires triggering the qahm_cron_data_manage scheduled event via wp-cron.php to invoke the deserialization sink against a planted queue file, but this endpoint requires no authentication and fires automatically on a two-minute schedule.	8.8	More Details
CVE-2026-66669	Cross-Site Request Forgery (CSRF) vulnerability in Suplugins Superb Addons: Blocks, Patterns & Theme Designer superb-blocks allows Cross Site Request Forgery.This issue affects Superb Addons: Blocks, Patterns & Theme Designer: from n/a through 4.2.4.	8.8	More Details
CVE-2026-122299	Dulwich before 1.2.20 contains a commit object parsing vulnerability where the read path in _parse_commit resolves a duplicate tree header to the last occurrence instead of the first, diverging from core git's resolution behavior, while Poetry 2.5.1 ships this version and uses dulwich by default for git dependency installation. Attackers can craft a commit object with two tree headers so that reviewers and CI using git see a benign tree while Poetry's dulwich-based checkout resolves to a different attacker-controlled tree containing malicious build scripts such as setup.py, resulting in unreviewed code execution on the install or build host.	8.8	More Details
CVE-2026-57853	DataGerry before 3.3.0 contains a server-side template injection vulnerability that allows authenticated attackers with base.docapi.template.add permission to store arbitrary Jinja2 payloads in the template_data field via POST /rest/docapi/template, which is later rendered in a non-sandboxed Jinja2 environment when a user calls GET /rest/docapi/template/<id>/render/<object_id>. Attackers can exploit the standard cycler.__init__.__globals__.os gadget chain to execute arbitrary operating system commands as the DataGerry web process user, confirmed as root in default Docker deployments, achieving remote code execution.	8.8	More Details
CVE-2026-104799	The Mobile builder plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.4.2 via the `wcfmmp_profile_settings()` REST handler exposed at `POST /mobile-builder/v1/wcfm-profile-settings`. This is due to a PHP loose-comparison logic flaw in the meta key allow-list check — `strpos( $key, 'mobile_builder' ) == 0` evaluates to `true` for any key that does *not* contain the substring `'mobile_builder'` because `strpos()` returns `false` on no match and `false == 0` is `true` in PHP — combined with a `permission_callback` (`user_permissions_check`) that grants access to any authenticated user by only verifying	8.8	More Details

	`$user->exists()`. This makes it possible for authenticated attackers, with Subscriber-level access and above, to pass an unsanitized `data` array via the `key` and `data` parameters directly to `update_user_meta()`, overwriting arbitrary user meta on their own account — including the `wp_capabilities` meta key — to grant themselves Administrator-level privileges.		
CVE-2026-11376	IBM MQ 9.2.0.0 through 9.2.0.44 LTS, 9.3.0.0 through 9.3.0.42 LTS, 9.4.0.0 through 9.4.0.26 LTS, 9.4.0.0 through 9.4.5.1 CD, and 10.0.0.0 through 10.0.0.5 LTS and CD could allow an authenticated attacker to cause a denial of service or potentially execute arbitrary code due to an integer overflow when processing subscription requests with crafted buffer size values.	8.8	More Details
CVE-2026-122133	Mistral Vibe before 2.25.5 on Windows contains an untrusted search path vulnerability that allows attackers to execute code by placing git.exe in a repository root. Attackers can lure users into opening a crafted repository so SessionLogger and ProjectContextProvider run the malicious git.exe at session start before any trust prompt.	8.8	More Details
CVE-2026-122134	Mistral Vibe before 2.25.7 contains a remote code execution vulnerability that allows attackers to run commands by configuring malicious Git clean or process filter drivers in a repository. When a user opens a crafted repository, ProjectContextProvider._fetch_git_status runs git status at startup, invoking the filters and executing commands with user privileges before any trust prompt.	8.8	More Details
CVE-2026-122135	Mistral Vibe before 3.0.3 contains a remote code execution vulnerability that allows attackers to run commands by abusing repository-configured gpg.program during project context collection. A crafted repository setting gpg.program and log.showSignature with a signed commit makes git log execute the attacker's program at session start, before any trust prompt.	8.8	More Details
CVE-2026-13292	IBM MQ 9.2.0.0 through 9.2.0.44 LTS, 9.3.0.0 through 9.3.0.42 LTS, 9.4.0.0 through 9.4.0.26 LTS, 9.4.0.0 through 9.4.5.1 CD, and 10.0.0.0 through 10.0.0.5 LTS and CD could allow an authenticated attacker to execute arbitrary code by injecting malicious environment variables through transfer request metadata.	8.8	More Details
CVE-2026-103002	GPUStack is an open-source GPU cluster manager for AI model serving and GPU instance provisioning. From 2.2.0 until 2.2.2, cluster_apiserver_proxy forwarded an authenticated non-administrator's requests to a selected Kubernetes cluster without a resource-level authorization check. The proxy used a reachable worker's Kubernetes ServiceAccount credentials, so the caller could read sensitive resources, create or modify workloads, or delete resources according to that ServiceAccount's permissions. Exploitation required a Kubernetes-provider cluster with a reachable worker, and attacker-controlled workloads could result in code execution in the target cluster. This issue is fixed in version 2.2.2.	8.8	More Details
CVE-2026-54372	VitaFit Android application (com.vt.vitafit) before 2.8.1.0 contains an insecure TLS/SSL certificate validation vulnerability that allows network-based attackers to intercept and modify HTTPS traffic by exploiting a custom X509TrustManager that trusts all certificates and a hostname verifier that accepts any hostname. Attackers can perform a man-in-the-middle attack to capture account sessions and health-related API data, and use a captured session to delete the account's authentication record and prevent legitimate login.	8.8	More Details
CVE-2026-121762	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 11.18.0.	8.8	More Details
CVE-2026-119744	Cendio ThinLinc contains an improper authentication vulnerability in its browser-based web client (tlwebaccess) that allows an authenticated attacker to impersonate any other user, including root, by exploiting flaws in multi-step authentication flows such as one-time passwords, login banners, or expired password prompts. Attackers can leverage this authentication bypass during the multi-step login process to gain unauthorized access to other user accounts, including administrative privileges, in versions from 4.1.0 through 4.20.0.	8.8	More Details
CVE-2026-48178	Out of bound access in PPC due to race condition in global variable access	8.8	More Details
CVE-2026-118193	The GiveWP – Donation Plugin and Fundraising Platform plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 4.19.1 via the `donor_default_user_role` parameter. This is due to the `sanitize_option_donor_default_user_role()` function applying only a narrow literal check against the string `'administrator'` rather than enforcing the plugin's own `give_get_donor_safe_user_roles()` allowlist on save, and due to the `give_core_settings_import_callback()` AJAX handler writing imported JSON directly into the `give_settings` option via `update_option()` without invoking the sanitize filter at all. This makes it possible for authenticated attackers with the GiveWP Manager role (holding the `manage_give_settings` capability) and above to configure donor registration to assign privileged WordPress roles — up to and including Administrator via the import path — to every new donor account created through the platform. Via the settings save path, the Administrator role is blocked but any other elevated role (Editor, Author, etc.) is accepted; via the Tools › Import JSON path, the sanitize filter is bypassed entirely, allowing the Administrator role itself to be stored and subsequently applied to all newly registered donor accounts.	8.8	More Details
CVE-2025-15702	The Cloud Blocks WordPress plugin through 1.1.8 does not perform any authorisation or sanitisation when storing block asset URLs, allowing unauthenticated users to store malicious scripts that are executed in the browser of any privileged user, such as an administrator, who opens the block editor.	8.8	More Details
	The Import and export users and customers plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 2.5.11 This is due to a non-atomic multi-option write sequence in the		

CVE-2026-120554	`ACUI_Cron::save_settings()` function, which persists `acui_cron_activated`, `acui_cron_configured_by`, `acui_cron_user_id`, and `acui_cron_path_to_file` before reaching the authorization gate that calls `wp_die()` when a non-promoter submits a role. This makes it possible for authenticated attackers holding a custom delegated role with `create_users` but without `promote_users` or `edit_users` to escalate their privileges to Administrator, provided a prior administrator cron-tab save exists and no successful save intervenes before the next unattended cron tick processes the attacker's repointed CSV file.	8.8	More Details
CVE-2026-82910	Improper Neutralization of Special Elements Used in a Template Engine ('Server-Side Template Injection') in MacroScreenRenderer in Apache OFBiz 24.09 before 24.09.08 on all platforms allows a remote authenticated attacker holding only the two view permissions of a control-servlet webapp (e.g. CATALOG_VIEW and OFBTOOLS_VIEW on /catalog, held by OFBiz's own shipped order-entry clerk role) to execute arbitrary operating system commands as the OFBiz service account with a single GET request, by placing an apostrophe followed by FreeMarker expression source in a screen link parameter value, because renderLink concatenates link parameter values verbatim between apostrophes into an unquoted, unescaped template-source string that is compiled and evaluated at render time, allowing the injected expression to reach the allow-listed FlexibleStringExpander.expandString call and, through a runtime-assembled Groovy interpolation, unsandboxed code execution. Users are recommended to upgrade to version 24.09.08, which fixes this issue.	8.8	More Details
CVE-2026-82912	Improper Neutralization of Special Elements Used in an Expression Language Statement ('Expression Language Injection') in EmailServices in Apache OFBiz 24.09 before 24.09.08 on all platforms allows a remote authenticated attacker holding only OFBTOOLS_VIEW and ACCOUNTING_VIEW, the two view-level permissions that open the Accounting application, to execute arbitrary operating system commands as the account running OFBiz, by submitting a ${groovy:...} expression as the bodyText or subject value to the shipped Send Per Email invoice form, because sendMailFromScreen passes those caller-supplied values through FlexibleStringExpander.expandString, which compiles and evaluates embedded Groovy on a class loader that carries none of the SecureASTCustomizer restrictions GroovyUtil.eval applies elsewhere, behind a service and request-map that declare no permission check beyond base authentication. Users are recommended to upgrade to version 24.09.08, which fixes this issue.	8.8	More Details
CVE-2026-82960	Improper Control of Generation of Code ('Code Injection') in ModelFormField in the Apache OFBiz cms plugin before 24.09.08 on all platforms allows a remote authenticated attacker holding only CMS content-editor access to execute arbitrary operating system commands as the OFBiz process user via a single HTTP POST request, by submitting a crafted caContentIdTo parameter to EditAddContent, because the CMS screen copies that parameter into a top-level context variable that is interpolated into a form field's use-when attribute and the resulting string is passed unvalidated to GroovyUtil.eval(), whose compile-time SecureASTCustomizer sandbox does not restrict runtime reflection, allowing a payload that closes the expanded string literal and invokes java.lang.Runtime via reflection. Users are recommended to upgrade to version 24.09.08, which fixes this issue.	8.8	More Details
CVE-2026-84183	Incorrect Authorization in the updateLayout simple-method in applications/content/minilang/layout/LayoutEvents.xml in Apache OFBiz 24.09 before 24.09.08 on all platforms allows a remote authenticated attacker holding only OFBTOOLS_VIEW and CONTENTMGR_VIEW to execute arbitrary commands as the OFBiz process user, by using updateLayout's authorization check — which validates only the fixed CONTENT_CREATE operation rather than an update permission on the actual Content record and an independently selected DataResource — to relink an existing RESPONSE-purpose Content record and convert an arbitrary, independently selected DataResource into an OFBIZ_FILE/FTL resource pointed at the OFBiz access log, poisoned via a crafted User-Agent header and evaluated through the normal authenticated showContent route. Users are recommended to upgrade to version 24.09.08, which fixes this issue.	8.8	More Details
CVE-2026-85627	Improper Neutralization of Special Elements Used in a Template Engine ('Server-Side Template Injection') in Apache OFBiz 24.09 before 24.09.08 on all platforms allows a remote authenticated attacker holding only a stock non-administrative account to execute arbitrary operating system commands as the OFBiz process user, by using the updateLayoutImage event, which writes DataResource fields with no permission check, to retype an attacker-created DataResource as an FTL template evaluating its own primary key, then using the resulting FreeMarker evaluation to plant an OFBiz Form Widget whose use-when attribute runs unsandboxed Groovy. Users are recommended to upgrade to version 24.09.08, which fixes this issue.	8.8	More Details
CVE-2026-71548	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to 7.15.2 and 8.10.2, AOR_Report::build_report_query_where incorporates a report editor's parameter_value when value_type=Field without sufficient validation. An authenticated user who can save a report can use SQL injection to read the entire SuiteCRM database. Disclosed data can include users.user_hash, OAuth2 tokens, CRM records, report definitions, and configuration data; the connector does not permit stacked queries, so direct write-through-injection is not supported. This issue is fixed in versions 7.15.2 and 8.10.2.	8.8	More Details
CVE-2026-69134	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to 7.15.2 and 8.10.2, the REST v4 JSON handler reads the pre-filter RAW_REQUEST value and relationship write helpers interpolate supplied field values into INSERT and UPDATE statements. The affected flow begins at $GLOBALS['RAW_REQUEST'] and uses set_relationship, SugarRelationship::addRow(), SugarRelationship::updateRow(), and contact_role to carry attacker-controlled data or authorization state into the security-sensitive operation. An authenticated user can inject SQL through relationship fields to read or alter database data and may reach file-write consequences when the database account has elevated privileges. This issue is fixed in versions 7.15.2 and 8.10.2.	8.8	More Details
CVE-2026-	The Cool Media Filter WordPress plugin through 1.0.1 does not perform any capability or nonce check when updating the capabilities of a role, allowing any authenticated user, such as a subscriber, to grant their own role	8.8	More

87784	administrator capabilities and take over the site.		Details
CVE-2026-85712	Chartbrew is an open-source web application that can connect directly to databases and APIs and use the data to create charts. Prior to 5.2.3, the shared project permission check trusted a caller-controlled team_id and let the teamOwner/teamAdmin branch continue without confirming that the target project belonged to that team. The vulnerable surface is project routes and related authorization checks that accepted user-controlled project identifiers. An authenticated user who is an owner or admin of their own team submits a victim project id together with the attacker's own team_id in the request body; default self-signup grants the required role on the user's own team. Authorization is evaluated against the attacker-selected team instead of the target project's team, and the update path mass-assigns the request body without a project field allow-list. The attacker needs a valid Chartbrew account, an owner or admin role on their own team, and a victim project identifier; requests without the body team_id trick are rejected. The attacker can re-parent the victim project into their own team, gain full read and write access, expose it publicly, remove password protection, and cause the victim to lose it; the shared delete route also permits cross-tenant deletion. This issue is fixed in version 5.2.3.	8.8	More Details
CVE-2026-120839	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Magepeople inc. WpTravelly tour-booking-manager allows PHP Local File Inclusion.This issue affects WpTravelly: from n/a through 2.3.8.	8.8	More Details
CVE-2026-88799	The MDJM Event Management and Mobile Events Manager WordPress plugins through 1.7.8.7 do not check ownership or capability on the identifier supplied to their client profile update, allowing any authenticated user, such as a subscriber, to change the password and email address of any other account including an administrator, resulting in a full account takeover.	8.8	More Details
CVE-2026-50240	A flaw was found in OpenShift Pipelines-as-Code (PAC). PAC does not verify whether the creator of a Repository custom resource has permission to create PipelineRuns. A namespace user with only Repository and Secret create/delete permissions can cause PAC to execute attacker-controlled PipelineRuns as the auto-provisioned pipeline ServiceAccount, which carries ClusterRole/edit by default. This results in namespace-scoped privilege escalation, enabling Secret read, resource creation/modification/deletion, and potential supply chain injection in CI/CD namespaces.	8.8	More Details
CVE-2026-116624	The Advanced Members for ACF plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.3.0 via the `acf[_amem_local_user_password]` parameter of the `[advanced-members-account-password]` shortcode form submission. This is due to a PHP operator-precedence bug in the `pre_update_value` function of `acf/fields/class-user-password.php` that assigns boolean `true` instead of the resolved user ID to `$user_id`, causing the `_can_edit()` authorization check to pass for any logged-in user via PHP loose equality, and causing `wp_update_user()` to cast `'ID' => true` to integer `1` — unconditionally targeting the primary administrator account. This makes it possible for authenticated attackers, with Subscriber-level access and above, to overwrite the password of user ID 1 (the site's primary administrator) with an attacker-chosen value, granting full administrative access to the site. The intended exclusion guard in `Account::process` that strips the password field before saving is defeated because `amem_save_all_fields()` re-reads the full field list from `amem()->submission` and silently overwrites the caller-supplied excluded fields array with an empty array, ensuring the password field is always processed.	8.8	More Details
CVE-2026-123490	Craft CMS from 5.8.17 before 5.11.2 contains a privilege escalation vulnerability because getOwners() applies caller criteria without cleansing the query configuration. Authenticated control panel users can invoke attacker-selected static PHP callables via crafted criteria to promote every account to administrator.	8.8	More Details
CVE-2026-120641	CGI versions before 5.00 for Perl return upload filenames with any client-supplied path, including ../ and Windows paths. The name returned for an uploaded file is the filename parameter of the part's Content-Disposition header, unchanged. An application that saves the upload under this name can be made to write outside the intended directory.	8.8	More Details
CVE-2026-123621	Usermin through 2.570 contains a path traversal vulnerability in mailbox/detachall.cgi that allows remote unauthenticated attackers to write files outside the temporary directory via unsanitized attachment filenames. Attackers can email attachments with ../ sequences in filenames, and when the recipient downloads all attachments, files like ~/.forward are overwritten, enabling command execution.	8.8	More Details
CVE-2026-123783	Skyvern through 1.0.56 contains a sandbox bypass vulnerability that allows authenticated users to execute code by reconstructing functions from raw bytecode with types.CodeType. Attackers can deploy scripts that evade the is_safe_script_code AST denylist and import blocked modules such as subprocess or socket to run code in the Skyvern server process.	8.8	More Details
CVE-2026-80301	Improper isolation in the Avast sandbox on Windows allows a local, low-privileged attacker executing inside the sandbox to access COM interfaces to the Task Scheduler service, escape containment, and execute code with elevated privileges outside the sandbox. The sandbox virtualizes file system and registry access but does not adequately restrict COM interface access to Task Scheduler. A process inside the sandbox can instantiate COM objects bound to Task Scheduler functionality and invoke methods to schedule and execute tasks on the host system. The Task Scheduler COM pathway is not blocked by the sandbox policy, allowing arbitrary code execution in the host security context. This escape vector bypasses the sandbox's intended process and file isolation boundaries and can be chained with other host-level privilege escalation techniques.	8.8	More Details
	The Interactive Real Estate – Floor Plan & Building Visualizer plugin for WordPress is vulnerable to Arbitrary File Upload in all versions up to, and including, 2.6.0 via the extract_zip_data function. This is due to missing		

CVE-2026-104913	capability check, nonce verification, and file extension or MIME type validation before copying attacker-supplied ZIP members to the uploads directory. This makes it possible for authenticated attackers, with subscriber-level access and above, to upload files that may be executable, which makes remote code execution possible. This vulnerability is only exploitable on sites where the plugin's Freemius Premium license or trial is active, as the sole gate in the handler is a site-level license check rather than a per-user capability check.	8.8	More Details
CVE-2026-80302	Insufficient isolation in the Avast sandbox file virtualization layer on Windows allows a local, low-privileged attacker executing inside the sandbox to write arbitrary files outside sandbox containment and execute code on the host. The sandbox virtualizes file system operations by intercepting write requests to protected system directories. However, the virtualization implementation fails to properly validate write targets in certain edge cases, allowing writes to bypass the virtualization redirection and reach the actual host file system in protected locations. An attacker can exploit this to overwrite executable files, system libraries, or startup configurations with arbitrary content, leading to code execution with host privileges on subsequent system operations or reboot.	8.8	More Details
CVE-2026-123836	In JetBrains Datalore before 2026.4 workspace collaborators could obtain the owner's SSH private key via Git backup	8.8	More Details
CVE-2026-118670	OHIF Viewers is a zero-footprint DICOM viewer with shared extension packages. From 3.5.0-beta.0 until 3.12.15, 3.13.7, and 3.14.0-beta.19, the dicom-pdf extension reads the attacker-controlled MIMETypeOfEncapsulatedDocument value in extensions/dicom-pdf/src/getSopClassHandlerModule.js and uses it as the Blob media type for the attacker-controlled EncapsulatedDocument bytes. When a victim opens Encapsulated PDF SOP Class 1.2.840.10008.5.1.4.1.1.104.1, extensions/dicom-pdf/src/viewports/OHIFCornerstonePdfViewport.tsx embeds the Blob URL in an object element. A Blob labeled as HTML is handled as HTML despite the application/pdf object hint, and the Blob inherits the OHIF origin, allowing embedded script to access session storage, authentication tokens, and same-origin PACS requests. The malicious DICOM object may be opened locally, uploaded to a shared PACS, or supplied by a DICOMweb source. This issue is fixed in source versions 3.12.15, 3.13.7, and 3.14.0-beta.19.	8.8	More Details
CVE-2026-107154	A session validation vulnerability has been identified in the SonicOS management interface, which in specific conditions could potentially enable a remote unauthenticated attacker to perform unauthorized operations.	8.8	More Details
CVE-2026-107155	A permissive cross-domain policy vulnerability has been identified in the SonicOS management interface, which in specific conditions could potentially enable a remote unauthenticated attacker to perform unauthorized operations.	8.8	More Details
CVE-2026-123993	Hisense VIDAA Smart TV firmware V0000.01.00a.P0220 contains an unauthenticated access vulnerability where a QA build of the Google Cobalt browser engine exposes the WebDriver automation server on TCP port 4444 across all network interfaces without any authentication or pairing requirement. A LAN-adjacent attacker can connect to the exposed WebDriver service to execute arbitrary JavaScript, read and exfiltrate sensitive localStorage data including ACR telemetry, MAC addresses, ad-service credentials, and location data, inject persistent content onto the display, and access the window.hisense native bridge to perform filesystem read/write and system-state operations.	8.8	More Details
CVE-2026-65960	Tetragon is an eBPF-based security observability and runtime enforcement project. Versions before 1.7.0 can use a Helm default that exposes the privileged Tetragon gRPC API through an unauthenticated TCP listener on localhost:54321. An attacker who can run or compromise same-node hostNetwork pods can reach the listener and invoke privileged methods without authentication. These methods can add, delete, or reconfigure tracing policies and change debug settings, potentially resulting in privilege escalation or container escape. Version 1.7.0 changes the default endpoint to a Unix-domain socket. Deployments that do not expose an unauthenticated TCP listener are not affected.	8.8	More Details
CVE-2026-33050	GeoNode is a geospatial content management system, a platform for the management and publication of geospatial data. Prior to 5.1.0, a crafted vector file layer name supplied during upload allows a low-privileged remote user to inject shell syntax and execute arbitrary operating-system commands on the GeoNode server. This issue is fixed in version 5.1.0.	8.8	More Details
CVE-2026-110525	The MCB WordPress plugin through 1.0.0 does not sanitise or escape request header values before storing them and later rendering them in the administrator statistics grid, allowing unauthenticated attackers to store malicious JavaScript that executes in an administrator's browser session when the statistics page is viewed.	8.8	More Details
CVE-2026-121958	FreeRDP through 3.32.1 has a heap out-of-bounds write in the RDPGFX client because the delete_surface callback truncates surface hash keys to 16 bits, leaving the surface table inconsistent so HashTable_GetKeys writes past its allocated key array. A malicious or man-in-the-middle RDP server can exploit this by creating surfaceId 0xFFFF, closing the RDPGFX channel, sending repeated DELETESURFACE PDUs, and then sending ENDFRAME or RESETGRAPHICS.	8.8	More Details
CVE-2026-33944	Dolibarr is an open-source enterprise resource planning and customer relationship management application. Prior to 22.0.5 and 23.0.1, there is a SQL injection vulnerability in the Third Party company update functionality. The application concatenates the localtax1_value and localtax2_value properties into an SQL UPDATE statement without numeric conversion or other appropriate sanitization. An authenticated user with Third Party create or edit permission can submit crafted lt1 or lt2 POST parameters to read sensitive database information, including password hashes, API keys, and business data, or modify third-party records. This issue is fixed in versions 22.0.5	8.8	More Details

	and 23.0.2.		
CVE-2026-113663	AG2 is an open-source AgentOS. From 0.13.2 until ag2 1.1.1, and from autogen 0.13.2 to 0.14.1, SandboxShellTool configurations using allowed=[...] or readonly=True rely on ShellAdapter._filter and contains_shell_operator in ag2/tools/sandbox/filter.py and ag2/tools/sandbox/adapter/shell.py to validate a command prefix and reject selected shell syntax. The filter omits newline and carriage-return separators, while the accepted raw string is passed to sh -c, allowing an attacker-influenced agent command to execute an additional arbitrary statement. With the default LocalEnvironment backend, the injected statement runs as a host subprocess with the privileges of the agent process and can affect confidentiality, integrity, and availability. This issue is fixed in ag2 version 1.1.1.	8.8	More Details
CVE-2026-120841	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Magepeople inc. WpTravelly tour-booking-manager allows PHP Local File Inclusion.This issue affects WpTravelly: from n/a through 2.3.8.	8.8	More Details
CVE-2026-116786	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to 1.11.2, sofia_handle_sip_i_refer() placed raw Refer-To URI parameters and headers inside a sip_invite_params channel-variable block passed to switch_ivr_originate(). The originate parser treated a comma in the attacker-controlled value as a variable separator, allowing an authenticated caller on a bridged call to inject arbitrary variables into a newly originated leg. An injected execute_on_originate value could invoke the system dialplan application before answer and execute operating-system commands with the FreeSWITCH process privileges. SIP REFER is enabled by default, and the sender needs only a registered account and a call that takes the off-box transfer path, not administrative or Event Socket access. This issue is fixed in version 1.11.2.	8.8	More Details
CVE-2026-17190	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to execute arbitrary JavaScript due to cross-site scripting. HTML content supplied by a provider is not sufficiently sanitized before it is displayed, which could allow script content to run in the user's browser.	8.7	More Details
CVE-2026-118045	The Ever Accounting WordPress plugin before 2.3.3 does not restrict the file path supplied to its CSV import routine to an allowed directory, allowing users with its custom Accounting Manager role (which does not have administrator privileges) to delete arbitrary files on the server, such as wp-config.php, which takes the entire site offline.	8.7	More Details
CVE-2026-17332	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote attacker to bypass security restrictions due to improper certificate validation.	8.7	More Details
CVE-2026-54142	OpenHuman is an open-source agent harness available as a desktop application and Rust library. Before 0.57.13, background synchronization for connected services such as email, Slack, and Notion stores raw external content and later places it in the model context of autonomous background agents without neutralizing embedded instructions. ApprovalGate treats tool calls without an interactive chat context as pre-authorized automation, so attacker-authored content processed during a background tick can influence the model to invoke Composio actions without presenting an approval request. An attacker who can deliver content to a connected account can use this path to send or forward data, post messages, create or modify third-party content, or disclose information from OpenHuman memory and integrations. The issue requires an active integration and successful model interpretation of the injected instructions. This issue is fixed in version 0.57.13.	8.7	More Details
CVE-2026-119432	A stored cross-site scripting (XSS) vulnerability exists in the Foxit Workspace's file share preview functionality. An attacker could upload a crafted file and share it with a victim. When the victim opens or previews the file, the embedded script executes in the application's origin, potentially accessing locally stored credentials and enabling credential theft.	8.7	More Details
CVE-2026-17291	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to perform account takeover due to an open redirect vulnerability. The redirect address used during OAuth 2.0 sign-in is not sufficiently validated, which could allow authentication results to be sent to an attacker-controlled location.	8.7	More Details
CVE-2026-17356	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a local attacker to obtain sensitive information due to the use of a hard-coded cryptographic key.	8.7	More Details
CVE-2026-122266	Improper isolation of shared resources in aws-network-policy-agent in Amazon EKS Network Policy Agent before 1.3.7 (VPC CNI before 1.22.3) might allow an authenticated adjacent user to bypass NetworkPolicy ingress enforcement on co-located pods via eBPF conntrack map poisoning using crafted AF_PACKET frames. To remediate this issue, users should upgrade to Amazon VPC CNI Managed Add-on v1.22.3 or later (which includes Network Policy Agent v1.3.7).	8.7	More Details
CVE-2026-121966	Traefik 2.x before 2.11.60 and 3.x before 3.7.16 sends ForwardAuth subrequests (and, in 3.7, Ingress NGINX auth-url requests) through an auth-server connection pool shared by all clients, exposing connection-bound NTLM or Negotiate authentication. An unauthenticated attacker can reuse another user's authenticated connection, receiving the victim's identity via authResponseHeaders to access backends as that user.	8.7	More Details
CVE-2026-	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to execute arbitrary JavaScript in the victim's browser due to cross-site scripting. User-supplied input is	8.7	More

16709	not properly neutralized when a web page is updated, so script content could run in another user's session.		Details
CVE-2026-57567	Readest is a modern, feature-rich ebook reader designed for seamless cross-platform access and an intuitive reading experience. In affected desktop Tauri builds prior to 0.11.10, the apps/readest-app/src-tauri/src/transfer_file.rs commands download_file and upload_file accepted a webview-controlled file_path and passed it to File::create or File::open without checking the Tauri filesystem scope, rejecting absolute paths, or blocking parent-directory traversal. The commands were registered in the global invoke handler for the main, updater, and reader-* windows, so JavaScript executing in the privileged application origin could write attacker-controlled content to any path writable by the process or read and send any path readable by the process. Exploitation requires JavaScript execution in that privileged origin, such as through an application XSS or compromised renderer; whether book-embedded JavaScript can reach the parent origin was not established. The write primitive can overwrite trusted or startup files, while the read primitive can expose keys, tokens, and application secrets. This issue is fixed in version 0.11.10.	8.6	More Details
CVE-2026-88981	Kubeflow Pipelines enables users to build and deploy portable, scalable machine learning workflows. Prior to 2.18.0, the frontend artifact download path for source=s3 or source=minio accepts providerInfo.Params.endpoint, and the archived pod-log path accepts S3-compatible endpoint metadata from workflow status, without requiring those endpoints to match operator-controlled storage configuration. In the shipped authorization-disabled standalone configuration, an unauthenticated caller can make the shared ml-pipeline-ui pod connect to arbitrary reachable hosts and return response data; requests may also reveal an access-key identifier when signed with configured object-store credentials. Multi-user secret-backed metadata remains restricted to the server namespace. This issue is fixed in version 2.18.0.	8.6	More Details
CVE-2026-110532	The Mail Mage WordPress plugin through 0.0.25 does not properly sanitise and escape a user-supplied value before using it in a SQL statement, allowing unauthenticated attackers to perform SQL injection attacks.	8.6	More Details
CVE-2026-88980	Kubeflow Pipelines enables users to build and deploy portable, scalable machine learning workflows. Prior to 2.18.0, the frontend GET /artifacts/get route accepts source=http or source=https with caller-controlled bucket and key values, and isAllowedResourceName permits an all-digit decimal host that the URL parser converts to an IPv4 address. The default ALLOWED_ARTIFACT_DOMAIN_REGEX and authorization-disabled standalone configuration allow an unauthenticated caller to fetch internal HTTP resources and receive their response body. In the authenticated multi-user configuration, the same destination-validation defect is reachable by a low-privilege tenant with a valid identity and authorized namespace. Cloud credential disclosure depends on reachable metadata services and attached roles, and the issue does not establish IMDSv2 bypass or credential access when metadata is blocked. This issue is fixed in version 2.18.0.	8.6	More Details
CVE-2026-73856	ModSecurity is an open source, cross platform web application firewall (WAF) engine for Apache, IIS and Nginx. From 3.0.0 until 3.0.17, src/transaction.cc compares a response Content-Type value against SecResponseBodyMimeType entries case-sensitively. A mixed-case response media type that is semantically equivalent to a configured lowercase type can therefore be treated as unconfigured, causing ModSecurity to skip RESPONSE_BODY inspection. An unauthenticated requester can then receive response content that a phase 4 rule would otherwise block, including sensitive error or debug data. This issue is fixed in version 3.0.17.	8.6	More Details
CVE-2026-104269	ModSecurity is an open source, cross platform web application firewall (WAF) engine for Apache, IIS and Nginx. From 3.0.0 until 3.0.17, ModSecurity's multipart parser does not apply the RFC 2231 filename* parameter precedence used by common Go, Python, Node.js, and Java application parsers. A Content-Disposition header can provide a benign filename parameter for ModSecurity and a different encoded filename* value that the backend prefers, causing MULTIPART_FILENAME rules and the application to make security decisions on different names. Applications that use the backend-selected name for storage, extension checks, or content-type inference can therefore receive a filename that bypassed WAF inspection. PHP's native multipart parser is not affected by this discrepancy. This issue is fixed in version 3.0.17.	8.6	More Details
CVE-2026-33379	A user with any role, including Viewer or a service account with no permissions, can create, externally publish, and delete dashboard snapshots (missing authorization). Only Grafana OSS and Grafana Enterprise 12.4 are affected; earlier versions and Grafana 13 are not.	8.5	More Details
CVE-2026-17382	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to a path traversal vulnerability.	8.5	More Details
CVE-2026-17365	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to server-side request forgery.	8.5	More Details
CVE-2026-17380	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to access sensitive information belonging to other tenants due to improper validation of a path parameter. A path value in a request is not sufficiently validated, which could allow a user to reach data outside their own tenant.	8.5	More Details
CVE-2026-17381	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to improper authorization validation using user-controlled keys.	8.5	More Details

CVE-2026-49272	OAuthLib is an implementation of the OAuth request-signing logic for Python 3.6+. From 3.3.0 until 4.0.1, OAuthLib's RFC 8628 device workflow does not require DeviceCodeGrant.validate_token_request to check that the device_code parameter is present and valid. A caller whose client request is accepted by the configured validator and who knows a valid client ID enabled for the device workflow can submit a missing or bogus device code to the token endpoint and obtain a bearer token without completing device authorization. This issue is fixed in version 4.0.1.	8.5	More Details
CVE-2026-17384	IBM API Connect 10.0.8.0 through 10.0.8.12 could allow a remote authenticated attacker to obtain sensitive information due to a server-side request forgery vulnerability.	8.5	More Details
CVE-2026-122308	Kyverno before 1.19.2 contains an authorization bypass vulnerability in the Generation Handler that allows users with create/update permissions to trigger synchronized generate policies by spoofing internal generate.kyverno.io labels. Attackers can label a ConfigMap as managed-by kyverno with crafted policy, rule, and trigger labels to clone sensitive Secrets from restricted namespaces into their own namespace.	8.5	More Details
CVE-2026-123786	Agenta before 0.122.5 contains a server-side request forgery vulnerability that allows workspace members with workflow edit rights to redirect workflow invocations by setting arbitrary revision URLs. Attackers can capture the attached secret-resolve Authorization token to read provider secrets from the vault API, or reach internal and cloud metadata addresses.	8.5	More Details
CVE-2026-17385	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to server-side request forgery.	8.5	More Details
CVE-2026-17388	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to broken object-level authorization.	8.5	More Details
CVE-2026-17397	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to server-side request forgery.	8.5	More Details
CVE-2026-122316	Kyverno from 1.17.0 before 1.19.2 contains a missing authorization vulnerability in the mutate-existing background processor that allows namespaced tenants to modify resources outside their namespace. Attackers can create a NamespacedMutatingPolicy targeting Namespace objects or victim-namespace resources via CEL expressions, making the background-controller ServiceAccount strip Pod Security labels cluster-wide.	8.5	More Details
CVE-2026-17404	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to server-side request forgery.	8.5	More Details
CVE-2026-17407	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to execute arbitrary SQL commands due to SQL injection. Values received during sign-in are not properly neutralized before being used in a database query, which could allow SQL commands to run.	8.5	More Details
CVE-2026-17398	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to server-side request forgery.	8.5	More Details
CVE-2026-17406	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to server-side request forgery. Address checks can be bypassed, which could allow the server to reach destinations that should be blocked.	8.5	More Details
CVE-2026-63111	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to 7.15.2 and 8.10.2, the V8 module API lacks module-level authorization and permits a low-privileged user to create SchedulersJobs records with attacker-controlled target values. The affected flow begins at /Api/V8/module and uses SchedulersJobs, target, cron.php, and url:: to carry attacker-controlled data or authorization state into the security-sensitive operation. Cron.php later executes the queued job with system privileges, and the url:: target makes server-side requests to internal or external hosts, can follow redirects, can persist as a recurring job, and may expose internal services. This issue is fixed in versions 7.15.2 and 8.10.2.	8.5	More Details
CVE-2026-17287	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to server-side request forgery. User-supplied addresses are not sufficiently validated, so the server could be made to send requests to unintended destinations and return the results.	8.5	More Details
CVE-2026-16880	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to path traversal.	8.5	More Details
CVE-2026-16912	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to server-side request forgery.	8.5	More Details

CVE-2026-17108	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to server-side request forgery.	8.5	More Details
CVE-2026-17172	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to bypass security restrictions due to improper authentication. Information supplied by the client is not sufficiently verified, which could allow a caller to impersonate another party.	8.5	More Details
CVE-2026-17187	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to improper validation of user-supplied URLs.	8.5	More Details
CVE-2026-17188	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to server-side request forgery. When service definitions are imported, references to external resources are not sufficiently restricted, so the server could be made to request resources it should not access.	8.5	More Details
CVE-2026-17228	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to server-side request forgery. Destination restrictions on outbound requests can be bypassed, which could allow the server to retrieve content from unintended resources.	8.5	More Details
CVE-2026-102340	Telepresence enables local development against a remote Kubernetes or OpenShift cluster. Prior to 2.31.0, the Traffic Manager gRPC API on port 8081 accepts unauthenticated cluster-network callers, ArriveAsClient stores a caller-supplied Namespace using only the ManagesNamespace manager watchlist check, and CreateIntercept can target any managed namespace without checking the session's Kubernetes RBAC. An attacker operating any pod with network access to the manager can register in an arbitrary managed namespace, create service intercepts, receive intercepted traffic, and obtain the victim pod's complete container environment, including secrets, tokens, and API keys. The default cluster-wide deployment manages all namespaces. This vulnerability is fixed in 2.31.0.	8.5	More Details
CVE-2026-17352	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to server-side request forgery.	8.5	More Details
CVE-2026-17334	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to improper authorization via user-controlled keys.	8.5	More Details
CVE-2026-17288	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to server-side request forgery.	8.5	More Details
CVE-2026-17290	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to create unauthorized user accounts due to improper verification of cryptographic signatures. Identity information from a login provider is accepted without its signature being fully verified, so forged identity data could be used to create accounts.	8.5	More Details
CVE-2026-17293	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to modify user profile information due to broken object-level authorization. Access checks do not confirm that the user is permitted to change the targeted profile.	8.5	More Details
CVE-2026-17294	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to server-side request forgery.	8.5	More Details
CVE-2026-11724	IBM MQ 9.2.0.0 through 9.2.0.44 LTS, 9.3.0.0 through 9.3.0.42 LTS, 9.4.0.0 through 9.4.0.26 LTS, 9.4.0.0 through 9.4.5.1 CD, and 10.0.0.0 through 10.0.0.5 LTS and CD could allow an authenticated attacker to execute arbitrary code on a Managed File Transfer agent host due to improper validation of metadata used during script execution.	8.5	More Details
CVE-2026-17325	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to improper validation of user-supplied URLs.	8.5	More Details
CVE-2026-17327	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to server-side request forgery.	8.5	More Details
CVE-2026-17328	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to improper input validation. Input checks are incomplete, which could allow them to be bypassed.	8.5	More Details
CVE-2026-17330	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to server-side request forgery.	8.5	More Details
CVE-			

2026-69044	In the Samsung GPU driver, improper reference count handling during command submission can lead to memory corruption.	8.4	More Details
CVE-2026-69066	Memory corruption in GPU driver due to improper validation of VMID reservation.	8.4	More Details
CVE-2026-123962	In FreedomBox before 26.15, unprivileged user accounts can read/write files for which they lack permissions by setting the authorized_keys file to be a symlink. NOTE: FreedomBox is a Debian Pure Blend, which means that it distributes its software through Debian repositories.	8.4	More Details
CVE-2026-82033	DeepSeek Harness prior to 0.1.2-alpha.2, and specifically commit 3e24087, contains a missing authentication vulnerability in its web profile HTTP and WebSocket RPC control plane, allowing any local process, including those running as a different OS user, to reach unauthenticated session methods such as session.create and session.prompt. Attackers can invoke session.prompt to trigger the agent's bash and filesystem tools, achieve arbitrary command execution as the victim user using their configured model credentials, intercept live session traffic and logs over the event mux stream, and bypass human tool-approval checks via POST /api/respond by matching only rpcId, approvalId, and sessionId values broadcast over the ungated stream.	8.4	More Details
CVE-2026-54375	VitaFit Android application (com.vt.vitafit) before 2.8.1.0 contains an insecure session management vulnerability that allows attackers to extract or intercept unencrypted m_session_id tokens stored in application backups, which remain valid for ten years. Attackers can use a stolen session token to read and modify the victim's account or delete the account's authentication record, preventing the legitimate owner from logging in again.	8.4	More Details
CVE-2026-49393	OpenHuman is an open-source agent harness available as a desktop application and Rust library. Before 0.56.0, the core server protects HTTP POST requests to /rpc with bearer middleware but exposes Socket.IO rpc:request and chat:start handlers without equivalent transport or handler-level authentication. A local unauthenticated client can connect to the Socket.IO namespace and dispatch requests through the same protected controller path that rejects a missing bearer on /rpc. Depending on the selected method, the attacker can read configuration or health data, start agent flows, interact with integrated account APIs, alter local data, or stop and restart services. This issue is fixed in version 0.56.0.	8.4	More Details
CVE-2026-123323	In JetBrains YouTrack before 2025.3.170763, 2026.1.14150, 2026.2.19656 improper URL validation in the app widget host allowed apps to send REST requests without user confirmation	8.4	More Details
CVE-2026-110935	The PFI plugin framework deployment routine does not validate path components when extracting archive entries to the local plugin repository. Archive entries containing relative path segments such as '..' are not rejected, allowing an unauthenticated local attacker to write files outside the plugin repository to arbitrary locations accessible with the current user's permissions which could result in full system compromise.	8.4	More Details
CVE-2026-110022	The PFI plugin framework deploys executable assemblies (DLLs) from a signed plugin package into the local plugin repository and loads them via reflection, but the deployment routine processes archive entries that were never covered by the signature verification. An unauthenticated local attacker can replace an unsigned DLL outside the signed prefix in the archive passes verification and overwrites the legitimate signed assembly at the same destination path. The plugin loader then instantiates the attacker-supplied code without any additional integrity check resulting in a full compromise of the affected systems.	8.4	More Details
CVE-2026-61648	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to 7.15.2 and 8.10.2, a user-controllable Multi report condition passes parameter_value through unencodeMultienum() and concatenates the result into a SQL WHERE clause. Although securexss() normally entity-encodes quotes, an input prefixed with an XSS payload makes AntiXSS select a processed string instead of the encoded backup, allowing a literal quote to reach the database. A low-privileged user with AOR Reports access can read arbitrary tables through time-based or UNION-based SQL injection and can consume database connections with delay expressions. This issue is fixed in versions 7.15.2 and 8.10.2.	8.3	More Details
CVE-2026-61653	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to 7.15.2 and 8.10.2, modules/Campaigns/PopupCampaignRoi.php interpolates $_REQUEST['id'] into SQL. Although securexss() normally entity-encodes quotes, an input prefixed with an XSS payload makes AntiXSS select a processed string instead of the entity-encoded backup, allowing a literal quote to reach the query. An authenticated user with Campaigns access can perform time-based blind SQL injection against arbitrary database tables. This issue is fixed in versions 7.15.2 and 8.10.2.	8.3	More Details
CVE-2026-17324	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote attacker to access sensitive configuration data and perform unauthorized actions due to missing authentication for a critical function.	8.3	More Details
CVE-2026-123998	Hisense VIDAA Smart TV firmware V0000.01.00a.P0220 contains an authentication bypass vulnerability in its remote-control MQTT broker on TCP port 36669, which accepts publicly documented default credentials and an ineffective 4-digit pairing PIN with no rate limiting or lockout, allowing a brute force of the entire code space in about five seconds, while some actions require no pairing at all. A LAN-adjacent attacker can exploit this to inject key events, change volume, switch input sources, enumerate inputs, launch arbitrary installed applications, and monitor pairing activity, posing a significant risk in hotel deployments where untrusted LAN access is common.	8.3	More Details

CVE-2026-69140	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to 7.15.2 and 8.10.2, GetLatestRevision.php interpolates get_latest_for_id directly into an SQL UPDATE statement. Although securexss() normally entity-encodes quotes, an input prefixed with an XSS payload makes AntiXSS select a processed string instead of the encoded backup, allowing a literal quote to reach the query. A low-privileged user with Documents module access can disclose database data and mass-update linked_documents records, while stacked statements and arbitrary DROP or INSERT operations are not supported by this vector. This issue is fixed in versions 7.15.2 and 8.10.2.	8.3	More Details
CVE-2026-107903	Joomla Extension - balbooa.com - Stored XSS in reviews via inconsistent sanitization in Gridbox < 2.20.5.0	8.3	More Details
CVE-2026-54140	OpenHuman is an open-source agent harness available as a desktop application and Rust library. Before 0.57.13, OpenHuman places names, descriptions, titles, and parameter definitions returned by configured external MCP servers into the agent model context without neutralizing instructions or bounding the descriptive fields. The McpRemoteTool records produced by list_tools preserve this remote content, while tool filtering considers the tool name and the prompt-injection detector screens user messages rather than MCP definitions. A malicious or compromised MCP server can therefore return a poisoned description that is evaluated on every agent turn and may direct the model to invoke other available tools, disclose accessible data, or perform unauthorized actions without a separate malicious user message. The issue affects users who configure an attacker-controlled or compromised MCP server. This issue is fixed in version 0.57.13.	8.3	More Details
CVE-2026-19121	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow an authenticated attacker to gain unauthorized access due to improper authorization. Tenant context is not sufficiently verified against the authenticated user, which could allow access to another tenant's resources.	8.3	More Details
CVE-2026-61651	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to 7.15.2 and 8.10.2, the get_end_date action in Projects Controller concatenates an authenticated caller's task_id value into a SQL query without parameterization. A low-privileged user can use blind SQL injection to enumerate the database schema and extract credentials, customer records, and other database contents. This issue is fixed in versions 7.15.2 and 8.10.2.	8.3	More Details
CVE-2026-87040	The nRF link-layer receive paths of the open-source Bluetooth LE Controller did not validate the on-air LENGTH field of a received PDU against the maximum receive length that was used to program the radio. isr_rx_pdu() in subsys/bluetooth/controller/ll_sw/nordic/lll/lll_conn.c enqueued any non-empty data PDU after only the sequence-number and (for encrypted links) MIC checks, and the corresponding isr_rx() handlers in lll_central_iso.c, lll_peripheral_iso.c, lll_sync_iso.c and lll_scan_aux.c did the same for ISO and extended-advertising PDUs. The nRF radio stores the received header verbatim and truncates only the payload at PCNF1.MAXLEN, so a frame declaring more octets than were configured leaves a node buffer whose len field describes more data than the buffer holds. An attacker within radio range that can emit a hand-crafted link-layer PDU — for a connection, any peer that establishes an unencrypted LE connection to a connectable advertiser; for CONFIG_BT_CTLR_SYNC_ISO, any broadcaster the device is synchronised to — can set the length byte up to 255 while the controller has programmed a much smaller maximum (lll->dle.eff.max_rx_octets, which is 27 until a Data Length Update, or the negotiated cis_lll->rx.max_pdu). No pairing, authentication or user interaction is required. On encrypted links the CCM MIC check normally rejects such a frame first, so the exposure is on unencrypted traffic, which is why the added check is placed after decryption. The unchecked length reaches hci_acl_encode() in subsys/bluetooth/controller/hci/hci.c, which performs net_buf_add(buf, pdu_data->len) followed by a memcpy() of that many bytes out of the node_rx pool element. Because CONFIG_BT_CTLR_DATA_LENGTH_MAX and CONFIG_BT_BUF_ACL_RX_SIZE both default to 27, this is an out-of-bounds read of up to roughly 228 bytes past the received PDU and a corresponding out-of-bounds write past the HCI ACL buffer into neighbouring buffers of the same pool; the tailroom test in net_buf_simple_add() is only enforced when CONFIG_NET_BUF_HARDENING (or CONFIG_ASSERT) is enabled. On the ISO paths the same unchecked length makes isoal_rx_append_to_sdu() read past the ISO node buffer and emit adjacent controller RAM to the host as ISO data. The practical result is remote memory corruption and controller crashes, plus disclosure of controller memory into the host data path. The fix rejects any received PDU whose length exceeds the value that was used to configure the radio reception. Note that lll_sync.c (periodic advertising sync reception) was not changed and still enqueues received PDUs without an equivalent bound.	8.3	More Details
CVE-2026-63215	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to 7.15.2 and 8.10.2, the REST API v4.1 get_entry_list method is vulnerable to time-based blind SQL injection when an authenticated caller simultaneously bypasses two independent security mechanisms. The advisory does not identify those controls more precisely, so their identities remain unspecified. Successful exploitation can extract sensitive database information. This issue is fixed in versions 7.15.2 and 8.10.2.	8.3	More Details
CVE-2026-105607	Joomla Extension - balbooa.com - Unauthenticated stored XSS in the "Recent Comments / Recent Reviews" widget in Gridbox < 2.20.5.0	8.3	More Details
CVE-2026-123675	A flaw has been found in OpenBMB Internet of Agents up to 9d78e88e47160eb42ee1ee8538c05e1c2c47877a. This affects the function execute_code of the file im_client/agents/tools/code_executor.py of the component Code Executor Tool. This manipulation of the argument filename/lang causes code 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.	8.3	More Details

CVE-2026-69141	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to 7.15.2 and 8.10.2, the CasesController action_get_kb_articles action interpolates $_POST['search'] into a CASE WHEN ... LIKE expression and the SQL WHERE clause. Although securexss() normally entity-encodes quotes, an input prefixed with an XSS payload makes AntiXSS select a processed string instead of the encoded backup, allowing a literal quote to reach the query. A low-privileged user with Cases module access can perform blind SQL injection and extract sensitive database information. This issue is fixed in versions 7.15.2 and 8.10.2.	8.3	More Details
CVE-2026-92704	SharpEmu is an experimental PlayStation 5 emulator for Windows and Linux. In version 0.0.3-release.3 and earlier, the repository-provided debugger frontend tooling is vulnerable while running. This tooling is not included in the release archives. The frontend exposes an HTTP API on 127.0.0.1:8765 without authentication or CSRF token. Its do_POST handler in tools/SharpEmu.DebuggerFrontend/debugger_frontend.py does not validate the Origin, Referer, Sec-Fetch-Site, or Host headers. The _read_json_body() function also accepts JSON sent with browser-simple content types instead of requiring application/json . A malicious page that can reach the loopback listener can send cross-origin requests to /api/launch , /api/command , and /api/connect . Chromium may require Local Network Access permission for pages served from public origins. Local-origin pages and other delivery paths are not consistently subject to this restriction. The /api/launch endpoint accepts an attacker-selected emulatorPath if it points to an existing file on the victim’s host. On POSIX systems, that file must also be executable. The endpoint additionally requires an existing ebootPath . The /api/command endpoint exposes debugger operations, including write-memory , set-register , and continue . The /api/connect endpoint can initiate outbound TCP connections. These operations can let an attacker execute an existing binary with the victim’s privileges, control the attached emulated process, or reach network services accessible from the host. DNS rebinding can additionally let the attacker read API responses interactively. This issue is fixed in version 0.0.3-release.3-patch.1	8.3	More Details
CVE-2026-123033	Authentication bypass in the HA heartbeat origin check in middlewared in TrueNAS SCALE before 25.10.8 (and in release trains before their respective fixes) allows an attacker on the same network segment to achieve unauthenticated full-administrator API access and execute commands as root. middlewared registers the HA peer-authentication hook (ha_permission) unconditionally, with no failover-licence or heartbeat-interface check. An unauthenticated connection whose TCP peer address is a hardcoded HA heartbeat address (169.254.10.1 or 169.254.10.2) and whose peer port is <= 1024 is granted a node credential that is authorized for every API method and treated as full administrator. Both conditions are properties of the attacker's own socket, and thus an attacker on the same layer-2 segment satisfies them without forging anything. The hook is present on non-HA, unlicensed, single-node Community Edition installations. The fix additionally requires that the connection terminate on the HA heartbeat listener (a local address/port the attacker cannot control).	8.3	More Details
CVE-2026-123018	A security flaw has been discovered in eosphoros-ai DB-GPT up to 0.8.2. This issue affects the function execute_code of the file code_utils.py of the component CodeAction. Performing a manipulation results in code injection. The attack can be initiated 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.	8.3	More Details
CVE-2026-102339	Telepresence enables local development against a remote Kubernetes or OpenShift cluster. Prior to 2.31.0, the Traffic Manager Tunnel gRPC streaming endpoint parses a session ID from the first bytes of a caller-controlled message in pkg/tunnel/message.go and passes it to state.Tunnel without verifying that the caller owns the active session. An attacker who obtains a valid active session ID through log leakage, cluster-internal channels, or the unauthenticated ArriveAsClient endpoint can attach a routed tunnel to that session and gain its network routing capabilities. UUID4 session IDs make cold brute force impractical. This vulnerability is fixed in 2.31.0.	8.2	More Details
CVE-2026-92698	FastNetMon is a high-performance DDoS detector and sensor. In version 1.2.9 and earlier, process_sflow_flow_sample() in src/sflow_plugin/sflow_collector.cpp passes the attacker-controlled sflow_raw_protocol_header_t.header_size to parse_raw_packet_to_simple_packet_full() as its trusted captured length without comparing it with the bytes remaining in the record. An inflated header_size creates a false end pointer beyond the received sFlow v5 UDP buffer, defeating the nested parser's bounds checks and causing an unauthenticated remote out-of-bounds read and process crash, with possible limited exposure of adjacent bytes through parsed flow fields. No fixed release is available as of this review.	8.2	More Details
CVE-2026-92695	FastNetMon is a high-performance DDoS detector and sensor. In version 1.2.9 and earlier, the live parse_packet() callback in src/pcap_plugin/pcap_collector.cpp is registered through pcap_loop and processes captured frames when pcap = on without checking packethdr->caplen. A short frame or an attacker-controlled IPv4 header length can make the parser dereference IP or transport headers beyond the captured bytes, causing an out-of-bounds read and process termination. No fixed release is available as of this review.	8.2	More Details
CVE-2026-122130	CESNET ipfixcol2 2.3.0 before 2.9.0 contains an integer overflow vulnerability in the Forwarder output plugin that allows unauthenticated IPFIX exporters to overflow a heap buffer by wrapping uint16_t message length counters. Attackers can send near-65535-byte data sets and large templates to a collector forwarding over TCP to crash it and perform 2-byte writes to attacker-influenced addresses.	8.2	More Details
CVE-2026-123491	Craft CMS 4.0.0 before 4.18.9 and 5.0.0 before 5.11.2 contains an SQL injection vulnerability in GraphQL eager-loading: arguments on eager-loadable nodes absent from the public schema are copied into EagerLoadPlan criteria without cleansing. Unauthenticated attackers can supply a parenthesized select argument to inject SQL expressions and read arbitrary database content, including password hashes and session tokens.	8.2	More Details
CVE-2026-	A length validation flaw in gdbserver's agent-expression parser allows an unauthenticated remote attacker to read uninitialized heap memory from the gdbserver process and cause a denial of service. Disclosed heap content	8.2	More

121996	includes addresses suitable for defeating ASLR in further exploitation.		Details
CVE-2026-17355	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information from internal network resources due to server-side request forgery. Destination checks on outbound requests can be bypassed, which could allow the server to reach internal systems that should be blocked.	8.2	More Details
CVE-2026-85743	FreeScout is a self-hosted help desk and shared mailbox. Prior to 1.8.230, multiple outbound paths in Helper::downloadRemoteFile(), Helper::checkPort(), Helper::sanitizeRemoteUrl(), MailboxesController.php, and ModulesController.php do not consistently enforce a sink-level restricted-host policy. An authenticated administrator, or another authenticated user permitted to change mailbox connection settings or trigger module update or installation paths, can supply attacker-controlled URLs or hosts. The independent download and port-test sinks can reach encoded or otherwise uncovered loopback and internal addresses. The redirect-validation bypass additionally requires a configured whitelist that permits the original and final hosts while a restricted internal host appears only as an intermediate redirect hop. No unauthenticated SSRF path is established. The server can consequently contact loopback and internal services, provide a blind internal port oracle, and retrieve internal HTTP responses into application-controlled download sinks. This issue is fixed in version 1.8.230.	8.2	More Details
CVE-2026-17358	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to bypass authentication across tenants due to improper authentication. Authentication checks are not sufficiently isolated between tenants, which could allow a user from one tenant to be accepted by another.	8.2	More Details
CVE-2026-92693	FastNetMon is a high-performance DDoS detector and sensor. In version 1.2.9 and earlier, parse_raw_packet_to_simple_packet_full() in src/simple_packet_parser_ng.cpp dereferences ipv6_extension_header_fragment_t when IpProtocolNumberIPV6_FRAG is present without first verifying that the eight-byte Fragment header remains. A crafted sFlow v5 RAW_PACKET_HEADER record can remotely reach this shared parser with the Fragment bytes omitted, causing an unauthenticated remote out-of-bounds read. The supplied harness detects the read under AddressSanitizer, but the advisory does not establish a production process crash. No fixed release is available as of this review.	8.2	More Details
CVE-2026-54376	VitaFit Android application (com.vt.vitafit) before 2.8.1.0 contains an insecure custom URI scheme vulnerability that allows a malicious application to intercept Fitbit login tokens by registering the same callback scheme (vitafit://vtio.cn). Attackers can capture the 30-day Fitbit authorization token with weight scope delivered in the callback URL to read, create, and delete the victim's weight and body-fat records via the Fitbit Body API.	8.2	More Details
CVE-2026-123301	In JetBrains IntelliJ IDEA before 2026.3 dOM-based XSS in the OpenAPI preview error view was possible	8.2	More Details
CVE-2026-93389	The LiteSpeed Cache plugin for WordPress is vulnerable to unauthenticated disclosure of sensitive WooCommerce customer data in all versions up to, and including, 7.9.1 With Cache REST enabled (the shipped default cache-rest=1), LiteSpeed stores WooCommerce Store API GET responses (/wc/store/v1/cart and /wc/store/v1/checkout) as PUBLIC cache objects and does not vary the cache on the Cart-Token or WooCommerce session. A shopper's personalized cart/checkout response is therefore served to any later, cookie-less and token-less client as an LSCache HIT. This makes it possible for unauthenticated attackers to read another shopper's billing and shipping details (name, company, street address, email, phone), cart contents and totals, and the shopper's live Cart-Token session JWT and nonce (enabling cart/checkout-session hijack), plus order_key on the checkout endpoint.	8.2	More Details
CVE-2026-116788	FreeSWITCH is an open-source software telecommunications platform. Before version 1.11.2, an integer underflow in switch_xml_decode() can cause an undersized heap allocation when an XML document declares an entity with an empty replacement value. Subsequent copying overruns the allocated buffer. An unauthenticated attacker who can reach a SIP profile with presence management enabled and DTD processing permitted can trigger the vulnerability through a crafted SIP PUBLISH request. Exploitation can corrupt heap memory and terminate the FreeSWITCH process, interrupting all active calls. This vulnerability is fixed in version 1.11.2.	8.2	More Details
CVE-2026-86442	The WP Event Manager WordPress plugin before 3.4.2 does not verify the ownership or the post type of a user supplied post identifier in its front-end event submission flow, allowing unauthenticated attackers to read and overwrite the content of arbitrary unpublished posts and pages, and to convert them into events.	8.2	More Details
CVE-2026-112340	Wazuh dashboard plugins from 4.9.0 before 4.14.9 contain an authorization bypass vulnerability that allows authenticated dashboard users to override the Manager API Authorization header via the /api/request proxy endpoint. Attackers can supply nested body.headers.Authorization values that replace the server-side session Bearer token, letting them act as another Manager API identity or send unauthenticated upstream requests.	8.2	More Details
CVE-2026-116783	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to 1.11.2, udptl_rx_packet() used a peer-controlled FEC entry count directly to fill five-entry FEC arrays in a mod_spandsp T.38 session. A larger count wrote sender-controlled error-recovery data beyond those arrays and persisted the oversized count for a later reconstruction pass. Any peer able to deliver UDPTL to an established T.38 fax session can reach the parser, including deployments using fax applications or a T.38 gateway. The memory corruption can crash FreeSWITCH and end every active call, although remote code execution has not been demonstrated. This issue is fixed in version 1.11.2.	8.2	More Details
CVE-2026-	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote attacker to obtain sensitive information due to	8.2	More

17323	XML external entity (XXE) injection.		Details
CVE-2026-71901	Improper Control of Resource Identifiers ('Resource Injection') vulnerability in Apache OFBiz. An authenticate user with access to sfa component can override the service to use on vcard import and access to other service. This issue affects Apache OFBiz: before 24.09.08. Users are recommended to upgrade to version 24.09.08, which fixes the issue.	8.1	More Details
CVE-2026-103935	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to 8.3.0, interface/forms/transfer_summary/new.php and interface/forms/functional_cognitive_status/new.php render stored transfer_to, code, and codetext values with text(), which uses ENT_NOQUOTES, inside double-quoted HTML value attributes. An authenticated clinical user can store a value containing a double quote that escapes the attribute and injects event-handler markup when another clinician opens the form. Successful exploitation can expose session data and protected health information or permit patient-record actions in the victim's session. This issue is fixed in version 8.3.0.	8.1	More Details
CVE-2026-53980	Charmbracelet wish before 2.0.5 contains a path traversal vulnerability in the git middleware (charm.land/wish/v2) that allows authenticated SSH users to escape the configured repository directory by supplying crafted repo paths that bypass a flawed forward-slash-count containment check in git.Middleware(). Attackers can use a single-depth path ../evil, or on Windows a payload ..\..\evil that defeats the slash-count guard entirely, to read or write arbitrary repositories outside the intended root via git-upload-pack, git-upload-archive, or git-receive-pack.	8.1	More Details
CVE-2026-119924	An out-of-bounds read in the TDS RPC procedure-name parser in the Babelfish for PostgreSQL extension versions 1.0-1.5, 2.1-2.15, 3.1-3.12, 4.0-4.8, 5.1-5.4 and in Amazon Aurora PostgreSQL with Babelfish might allow remote authenticated users to read adjacent process memory or cause a denial of service via a malformed TDS RPC request to the TDS port (default 1433). To remediate this issue, we recommend users upgrade to Babelfish for PostgreSQL extension versions 4.10, 5.6, 6.1 or later. As a workaround, restrict network access to the TDS port (default 1433). Customers using Amazon Aurora PostgreSQL with Babelfish should upgrade their cluster to Aurora PostgreSQL 13.9.16 (1.5.5), 13.23.3 (1.17.2), 14.6.16 (2.3.5), 14.17.8 (2.12.4), 14.18.6 (2.13.3), 14.19.5 (2.14.2), 14.20.5 (2.15.2), 14.22.3 (2.16.1), 14.23.1 (2.17.0), 15.10.8 (3.8.4), 15.12.8 (3.9.4), 15.13.6 (3.10.3), 15.14.5 (3.11.2), 15.15.5 (3.12.2), 15.17.3 (3.13.1), 15.18.1 (3.14.0), 16.8.8 (4.5.5), 16.9.6 (4.6.3), 16.10.5 (4.7.2), 16.11.5 (4.8.2), 16.13.3 (4.9.1), 16.14.1 (4.10.0), 17.4.8 (5.1.4), 17.5.6 (5.2.3), 17.6.5 (5.3.2), 17.7.5 (5.4.2), 17.9.3 (5.5.1), 17.10.1 (5.6.0), 18.3.4 (6.0.2), 18.4.1 (6.1.0) or later, and apply any pending maintenance to ensure they are on the latest patch.	8.1	More Details
CVE-2026-76077	ASN1SCC is an open source ASN.1 compiler for embedded systems. Prior to 4.7.0.1, the XER tokenizer NT() in asn1crt/asn1crt_encoding_xer.c, which is reached by all XER decode paths, copies tag characters into a fixed char Value[100] field without a length bound and reads input and lookahead bytes without checking the buffer count. A crafted XER message with an overlong tag can overwrite the tokenizer's stack frame, while a truncated tag or unterminated processing-instruction or comment sequence can read beyond the input and may cause a CPU spin. The flaws can disclose adjacent memory, corrupt stack data, crash or hang the decoder, and potentially permit code execution. This issue is fixed in version 4.7.0.1.	8.1	More Details
CVE-2026-75614	ASN1SCC is an open source ASN.1 compiler for embedded systems. Prior to 4.7.0.1, BitStream_DecodeConstraintWholeNumber in asn1crt/asn1crt_encoding.c reads enough bits for a constrained integer but does not reject values above the declared range when the encoded range is not a power of two. Generated uPER and ACN decoders for variable-size SEQUENCE OF, OCTET STRING, BIT STRING, and string values use the invalid result as a loop or copy length, so a crafted over-range size field can write beyond a destination buffer. Decoding untrusted affected data can corrupt heap or stack memory, cause a crash, or potentially permit code execution. This issue is fixed in version 4.7.0.1.	8.1	More Details
CVE-2026-114233	Incorrect Privilege Assignment in the Order Manager in Apache OFBiz 24.09 before 24.09.08 on all platforms allows an authenticated user who holds only order view permissions (ORDERMGR_VIEW), without ORDERMGR_UPDATE or any role on the order, to modify approved orders, changing a ship group's shipping address and shipment method or appending items with an overridden price, via the updateShipGroupShipInfo and appendOrderItem services. Users are recommended to upgrade to version 24.09.08, which fixes this issue.	8.1	More Details
CVE-2026-121997	A heap buffer overflow in gdbserver's QTDPsrc packet handler allows an unauthenticated remote attacker to achieve native code execution in the gdbserver process. The vulnerability results from a mismatch between a packet's declared source length and the actual data length, causing hex2bin to write beyond the allocated heap buffer.	8.1	More Details
CVE-2026-111822	Improper invalidation of cached authorizations vulnerability in Apache ActiveMQ, Apache ActiveMQ Runtime Config. After the runtime configuration plugin removes a principal's write grant on a destination, an authenticated connection opened before the change can keep sending to that destination, including through a new anonymous producer, while fresh connections and new explicit producers are denied. This issue affects Apache ActiveMQ: from 6.0.0 before 6.3.3, before 5.19.12; Apache ActiveMQ Runtime Config: from 6.0.0 before 6.3.3, before 5.19.12. Users are recommended to upgrade to version 6.4.0, 6.3.3 or 5.19.12, which fixes the issue.	8.1	More Details
CVE-2026-120635	CGI versions before 5.00 for Perl allow form fields to be smuggled past proxies and WAFs via multipart parsing that differs from the RFCs. The multipart/form-data parser matches the boundary anywhere rather than at the start of a line, uses the boundary without its leading -- for some client-supplied User-Agent values, finds the Content-Disposition name and filename inside the quoted values of other parameters, and corrupts parts when	8.1	More Details

	the boundary nears the 4096-byte read size.		
CVE-2026-121962	FreeRDP before 3.32.2 contains a heap buffer overflow in transport_default_read_pdu when handling partial Early User Authorization reads during PROTOCOL_HYBRID_EX CredSSP. A malicious RDP server can split the four-byte EUA result into short reads that advance the stream pointer beyond the 16 KiB allocation, causing an out-of-bounds write and client denial of service.	8.1	More Details
CVE-2026-123295	In JetBrains Hub before 2026.2.52519 enforced two-factor authentication could be disabled via the profile update endpoint	8.1	More Details
CVE-2026-17321	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to delete or overwrite arbitrary control-plane assets due to an insecure direct object reference.	8.1	More Details
CVE-2026-112208	A flaw was found in the Organization identity-first login flow of the Keycloak authentication server. Keycloak is an open-source identity and access management solution used to secure modern applications and services. The issue occurs when an attacker who belongs to multiple organizations initiates a login and then switches to a registration or password reset path. During this process, a flag indicating a successful login is not properly cleared when the user is removed from the session. An attacker can then provide a victim's username, and the system incorrectly treats the stale flag as proof of the victim's identity. This allows the attacker to bypass authentication and gain full access to the victim's account and connected applications.	8.1	More Details
CVE-2026-106714	Chewy for Android version 26.23.0 does not adequately validate the host of a product-details deep link before loading it in a Hybrid WebView. An attacker-controlled page with a /dp/<number> path can access the injected nma_petmd_bridge JavaScript interface and invoke getPetProfiles, disclosing a signed-in user's pet profile information after the user opens the crafted link.	8.1	More Details
CVE-2026-81828	Server-Side Request Forgery in SurveyWrapper in Apache OFBiz 24.09 before 24.09.08 on all platforms allows an authenticated back-office user holding catalog permission to cause the server to fetch and render attacker-controlled URLs — including internal network and cloud-metadata endpoints and local files via file:// — by setting an arbitrary URL as a product-store survey's template location, causing SurveyWrapper.getTemplate to call URL.openStream() on the resolved location and compile the fetched content as a FreeMarker template with no scheme or host validation, unlike the sibling widget location-loaders (ScreenFactory, FormFactory, GridFactory, MenuFactory, TreeFactory, ThemeFactory) which validate the resolved location before loading it. The fetched content is rendered into the HTTP response of any shopper who subsequently loads the affected product-store survey, making the disclosure non-blind. Users are recommended to upgrade to version 24.09.08, which fixes this issue.	8.1	More Details
CVE-2026-123184	An incorrect authorization vulnerability exists in the Altium 365 Git Service. The permission check performed when a user pushes to a project repository did not correctly evaluate the required access level, so the check passed for any user holding any level of access to the project. As a result, an authenticated user with view-only access to a project could write to that project's git repository. Read access was evaluated correctly and was not affected, and exploitation requires an authenticated account with existing access to the target project. The issue has been remediated in Altium 365 at the service level and no customer action is required. On-premise Altium Enterprise Server is not affected.	8.1	More Details
CVE-2026-123158	sshd in OpenSSH before 10.6p2 on Linux, when musl libc is used without PAM, lacks a workaround for a password authentication bypass (related to misinterpretation of whether a string is intended to be a password hash). For some configurations of accounts, any password between 256 and 1024 characters succeeds. An example of a platform using musl libc without PAM is Alpine Linux.	8.1	More Details
CVE-2026-103900	The WPJAM Basic plugin for WordPress is vulnerable to Privilege Escalation in versions up to, and including, 7.1 This is due to the WPJAM_User_Signup::signup() function unpacking attacker-supplied `data[args]` from the AJAX POST body and merging it via PHP array union into the payload passed to WPJAM_User::create(), whose internal whitelist (wpjam_pick) explicitly preserves the `role` key before it is handed to wp_insert_user(). The endpoint is registered as wp_ajax_nopriv_{provider}-signup with a nonce that is emitted on the public login page. This makes it possible for unauthenticated attackers to elevate their privileges to Administrator by creating a new user with an attacker-chosen role, provided a social-login provider is registered and open registration is enabled.	8.1	More Details
CVE-2026-123280	In JetBrains Datalore before 2026.2.4 unauthenticated users could execute code via published interactive reports	8.1	More Details
CVE-2026-107891	musl libc before 1.2.7, when an untrusted regular expression is used with regcomp, has multiple integer overflows, possibly leading to incorrect allocation sizes and out-of-bounds heap writes.	8.1	More Details
CVE-2026-13271	IBM MQ 9.2.0.0 through 9.2.0.44 LTS, 9.3.0.0 through 9.3.0.42 LTS, 9.4.0.0 through 9.4.0.26 LTS, 9.4.0.0 through 9.4.5.1 CD, and 10.0.0.0 through 10.0.0.5 LTS and CD Managed File Transfer could allow an authenticated attacker to obtain sensitive information or cause a denial of service due to improper restriction of XML external entity references in command queue processing.	8.1	More Details
	The Advanced Form Integration — Connect Forms to 300+ Apps plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 2.10.2 via deserialization of untrusted input . This makes it possible		

CVE-2026-104738	for unauthenticated attackers to inject a PHP Object. No known POP chain is present in the vulnerable software, which means this vulnerability has no impact unless another plugin or theme containing a POP chain is installed on the site. If a POP chain is present via an additional plugin or theme installed on the target system, it may allow the attacker to perform actions like delete arbitrary files, retrieve sensitive data, or execute code depending on the POP chain present. Exploitation requires that an administrator has previously configured at least one active NexForms integration (status=1) in the plugin's database table; in the free tier, only POST parameter keys containing the substrings 'name', 'email', 'first', or 'last' are routed to the vulnerable normalizer.	8.1	More Details
CVE-2026-122224	WebVirtCloud through commit bb920b0 contains a missing authorization vulnerability that allows low-privileged authenticated users to reach MigrateViewSet and CreateInstanceViewSet because no permission_classes are declared, so Django REST Framework defaults to AllowAny. Attackers can send requests to /api/v1/migrate/ or the compute instance create endpoint to migrate or undefine other users' virtual machines and create volumes and domains on any compute host.	8.1	More Details
CVE-2026-17386	IBM API Connect 10.0.8.0 through 10.0.8.12 could allow a remote attacker to gain full administrative control due to the use of a cryptographically weak pseudo-random number generator.	8.1	More Details
CVE-2026-58273	Rucio is a scientific data management framework. From 1.16.1 until 35.9.0, 38.6.0, and 41.0.0rc1, the /credentials/signurl endpoint reads X-Rucio-Account instead of the account stored in request.environ['issuer'] by token authentication. Any authenticated low-privilege user can supply root as the header value and pass the root-only get_signed_url permission check. The server then returns a presigned read, write, or delete URL for an attacker-selected object using stored S3, GCS, or Swift credentials, and X-Rucio-VO can select another tenant in multi-VO deployments. This permits data disclosure, modification, deletion, and cross-tenant access on cloud-backed RSEs. This issue is fixed in versions 35.9.0, 38.6.0, and 41.0.0rc1.	8.1	More Details
CVE-2026-17343	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to bypass authorization checks to access or modify sensitive information due to improper authorization.	8.1	More Details
CVE-2026-17326	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to bypass security restrictions due to improper authentication.	8.1	More Details
CVE-2026-123859	When identifier escaping is disabled through a non-default configuration, the write_pandas() data-loading functionality in the Snowflake Connector for Python and the Snowflake Connector for Python (Universal Core) did not escape DataFrame column names before including them in generated SQL, which could allow SQL injection. In both products, a crafted column name could have been used to chain additional SQL statements onto the generated statement, potentially allowing an attacker to read, modify, or delete other data accessible to the application's Snowflake role. Exploitation required an application to pass attacker controlled column names into this functionality. The fix is available in Snowflake Connector for Python version 4.8.1 and Snowflake Connector for Python (Universal Core) version 5.2.0. Users must upgrade manually.	8.1	More Details
CVE-2025-71456	vtenext before 25.02.2 contains an SQL injection vulnerability that allows authenticated low-privileged users to inject SQL by supplying a crafted fieldname parameter to modules/Fax/EditView.php. Attackers can read arbitrary database contents, including password reset tokens stored in vte_userauthtoken, to take over other user accounts.	8.1	More Details
CVE-2026-55368	h2o is an HTTP server with support for HTTP/1.x, HTTP/2 and HTTP/3. Prior to commit 48b7ae12107fd2b118e4641da49599e9aac8edd8, H2O's access-log formatter could write past its log-line buffer when an affected custom access-log format was configured. The allocation errors affected %{error}x, %q when the query string was empty, and numeric elements whose temporary terminating NUL reached the end of the buffer. A matching request could crash the server, while the effect of the one-byte NUL overwrite beyond a crash was not established. This vulnerability is fixed with commit 48b7ae12107fd2b118e4641da49599e9aac8edd8.	8.1	More Details
CVE-2026-114232	A flaw was found in the UserManagedPermissionService of the Keycloak authorization server. The UMA Protection API, which manages user permissions, fails to validate the resourceType field when a user creates a new policy. This allows an attacker to create a policy that applies to resources owned by other users, potentially leading to unauthorized access or modification of sensitive data across the entire realm.	8.1	More Details
CVE-2026-92857	Keycloak provides a Dynamic Client Registration feature that allows users with specific tokens to register their own applications. A flaw in how Keycloak validates these registration requests allows an attacker to create a malicious application that forges identity information. By mapping their own user profile details to protected fields like the user ID (sub) or intended audience (aud), an attacker can generate signed security tokens that make them appear to be a different user. This could allow an attacker to impersonate other users or gain unauthorized access to services that rely on these tokens for identity verification.	8.1	More Details
CVE-2026-16304	The WP Event Manager WordPress plugin before 3.4.2 does not properly validate ownership or the type of the user-supplied post identifiers processed by one of its frontend forms, allowing any user with a Subscriber account or above to reassign the authorship of arbitrary posts to themselves and to force them to be published. This results in content takeover and in the public disclosure of otherwise private or draft content, and requires the relevant frontend feature to be enabled.	8.1	More Details
	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to 8.3.0, library/classes/Controller.class.php allows explicit controller.php dispatch to controllers missing from		

CVE-2026-115573	CONTROLLER_ACL_MAP, and checkControllerAcl() returns without enforcing any permission for those entries. A low-privilege authenticated user can invoke C_X12Partner::edit_action_process() to create or alter insurance-routing hosts and credentials, or invoke C_PatientFinder::find_action_process() to enumerate patient names, dates of birth, and identifiers. The shared fail-open dispatcher root cause also exposes other administrative controllers that were intended to be reached through ACL-gated Practice Settings routes. This issue is fixed in version 8.3.0.	8.1	More Details
CVE-2026-123196	Authorizer before 2.4.2 contains a password reset poisoning vulnerability that allows unauthenticated attackers to control emailed link hosts by supplying x-authorizer-url gRPC metadata. Attackers can send this metadata to the gRPC port or a Grpc-Metadata-X-Authorizer-Url header through the REST gateway to capture reset or magic-link tokens and take over accounts.	8.1	More Details
CVE-2026-116617	The Motors – Car Dealership & Classified Listings Plugin plugin for WordPress is vulnerable to File Deletion in all versions up to, and including, 1.4.128 The vulnerability exists because `stm_save_user_extra_fields()`, hooked to `personal_options_update`, writes the attacker-controlled `stm_dealer_logo_path` parameter directly to user meta without an ownership check binding the submitted path to the submitting user — unlike the `stm_payment_status` and `stm_lost_password_hash` fields, this field is not gated by a `manage_options` or `edit_users` capability check. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete image files belonging to other users under `wp-content/uploads` — including other users' avatars, dealer logos, and uploaded media — by storing a crafted path via their own profile and then triggering `unlink()` through the become-dealer form on their author page. Note that the two path guards (`stm_mvl_is_path_within_uploads` and `stm_mvl_is_allowed_image_file`) do restrict the attack surface to files with an image extension that resolve within the uploads basedir; files outside that directory, such as `wp-config.php` or plugin PHP files, cannot be reached.	8.1	More Details
CVE-2026-61650	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to 7.15.2 and 8.10.2, the POST /Api/V8/module/{moduleName}/{id}/relationships/{linkFieldName} endpoint checks only view and list permissions before a one-to-many relationship writes a target record's foreign key, without enforcing the required edit permission. A low-privileged user can reassign records, alter ownership and security-relevant relationships, expand cross-user access, and manipulate workflows. This issue is fixed in versions 7.15.2 and 8.10.2.	8.1	More Details
CVE-2026-118267	The WP Data Access – App Builder for Tables, Forms, Dashboards, Charts & Maps plugin for WordPress is vulnerable to Incorrect Authorization leading to Privilege Escalation in all versions up to, and including, 5.5.89 This is due to the plugin's write endpoints (`wpda/app/update`, `wpda/app/delete`, `wpda/app/insert`) passing the attacker-supplied `key` and `val` parameters directly to `$wpdadb->update`, `$wpdadb->delete`, and `$wpdadb->insert` without enforcing the container's row-filter (`defaultWhere`) or per-column allow-list (`isSelected`) restrictions that are correctly applied on the read endpoints. This makes it possible for authenticated attackers, with Subscriber-level access and above, to write to arbitrary rows and columns outside the configured restrictions — including overwriting the `user_pass` field of the WordPress administrator account in `wp_users` — and subsequently authenticate as the administrator, achieving full site takeover. Exploitation requires an administrator to have published a Data App that enables write transactions (update, delete, or insert) for Subscriber-level or anonymous users, which is an explicitly advertised use-case of the plugin. Exploitation by unauthenticated attackers requires that the administrator has published a Data App whose rest_api.authorization is 'anonymous' and whose container has transactions.update (or delete/insert) enabled. On a default installation, where that is not configured, the vulnerability requires attackers with subscriber-level access and above.	8.1	More Details
CVE-2026-68984	In the Samsung Exynos NPU kernel driver, an integer overflow allows an unprivileged application to trigger memory corruption.	8.1	More Details
CVE-2026-92895	The Live2DWebCanvas plugin for WordPress is vulnerable to Arbitrary File Upload in all versions up to, and including, 2.2.1 via the download_one_file function. This is due to missing file extension whitelist and MIME type validation in download_one_file() when writing files derived from attacker-controlled manifest entries to the web-served plugin directory. This makes it possible for unauthenticated attackers to upload files that may be executable, which makes remote code execution possible when the plugin's apiType setting is configured as custom-local (self-hosted model mode), a non-default option that requires a paid license and prints the REST nonce and one-time session tokens into every front-end page.	8.1	More Details
CVE-2026-121939	Databasement before 1.10.9 contains an authentication bypass vulnerability in OAuthService::findOrCreateLocalUser() that links OIDC identities to local users by email without checking email_verified. Attackers can register an identity provider account with a victim's unverified email to log in as any user, including the super-admin, and retain access after password resets.	8.1	More Details
CVE-2026-123317	In JetBrains Ktor before 3.6.1 session forgery was possible via tampered encrypted session cookies	8.1	More Details
CVE-2026-104746	The Motors – Car Dealership & Classified Listings Plugin plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the stm_listings_ajax_save_user_data function in all versions up to, and including, 1.4.125 This makes it possible for authenticated attackers, with subscriber-level access and above, to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php). Although deletion is bounded to wp-content/uploads (preventing removal of wp-	8.1	More Details

	config.php), any authenticated Subscriber can trivially exploit this because the required AJAX nonce is printed on every front-end page and the handler's stm_user_avatar_path meta is writable by any logged-in user against their own account.		
CVE-2026-85736	Chartbrew is an open-source web application that can connect directly to databases and APIs and use the data to create charts. Prior to 5.2.3, connection creation or update stored attacker-chosen absolute SSL and SSH file paths, and later connection cleanup passed those stored paths to fs.unlink without a path restriction. The vulnerable surface is data-connection certificate and SSH-key cleanup when a connection is removed. A user with createOwn and deleteOwn permissions on their own team stores a target path in a connection and then deletes the connection to trigger cleanup; default self-signup grants teamOwner these permissions. The cleanup routine treats the stored SSL or SSH path as a managed certificate path and unlinks the referenced file; duplicateConnection provides a second advisory-identified trigger. The attacker must be able to create or update and then delete a connection on their own team. The default container runs Chartbrew as uid 0, while deployments with a less-privileged process are limited by that process's deletion permissions. The attacker can delete files such as /code/.env or application source, causing integrity loss and service disruption. This issue is fixed in version 5.2.3.	8.1	More Details
CVE-2026-124040	CivetWeb through 1.16, when built with USE_HTTP2 and enable_http2 on, contains a use-after-free vulnerability in handle_http2() that retains freed :method and :path pointers. Unauthenticated remote attackers can send a later HEADERS frame omitting these pseudo-headers to influence request method or path seen by access rules, or crash the server.	8.1	More Details
CVE-2026-102344	Lavish is the new editor for your HTML artifacts. Prior to 0.1.43, the lavish-axi loopback HTTP server did not authenticate requests or validate Host and Origin values on session, artifact, prompt, and polling routes. A website visited while the server is running can use DNS rebinding to send same-origin browser requests to the local service. POST /api/sessions accepts a caller-selected file path and returns its deterministic session key; GET /artifact/:key/index.html then returns the file contents, allowing disclosure of any file readable by the server process without an existing session. An attacker can also queue text through POST /api/:key/prompts for an active agent session when the artifact path is known or guessed. Visiting the attacker-controlled website is the required user interaction. This vulnerability is fixed in 0.1.43.	8.1	More Details
CVE-2026-123271	ChatCLI before v1.215.2 contains an improper validation vulnerability in the MCP OAuth login flow that uses server-supplied Protected Resource Metadata as the resource indicator without checking it matches the configured server URL. A malicious MCP server can declare another resource on the same authorization server, obtain the user's bearer token for it, and replay that token against the other resource.	8.0	More Details
CVE-2026-102523	MariaDB server is a community developed fork of MySQL server. From 10.11.1 until 10.11.19, 11.4.13, 11.8.9, 12.3.3, and 13.0.2, ALTER TABLE ... CONVERT ... PARTITION does not apply filename encoding to user-specified partition names before using them in filesystem path construction. An authenticated database user can use a partition name requiring filename escaping to make the conversion operate on table files the user is not authorized to access, allowing unauthorized table reads or modifications. This issue is fixed in versions 10.11.19, 11.4.13, 11.8.9, 12.3.3, and 13.0.2.	8.0	More Details
CVE-2026-110930	Codex Desktop for Windows does not correctly check quotation marks in project paths from Windows Explorer. If a user selects "Open project in ChatGPT" for an attacker-controlled library's child item, the path can add application startup arguments. These arguments can run attacker-controlled code with the current Windows user's permissions before sign-in or project trust approval.	8.0	More Details
CVE-2026-88801	The MDJM Event Management and Mobile Events Manager WordPress plugins through 1.7.8.7 do not check a capability or a nonce before creating a WordPress role from a name supplied in the request, and store that name without escaping it, allowing any authenticated user, such as a subscriber, to inject arbitrary web scripts which execute when an administrator opens one of the standard user management screens.	8.0	More Details
CVE-2026-123272	Mark3labs mcp-go before v1.2.1 contains an improper validation vulnerability in OAuthHandler.fetchServerMetadata that allows malicious MCP servers to obtain tokens for other resources by declaring arbitrary resources in well-known metadata. Attackers can declare a different MCP server as the RFC 8707 resource indicator, causing the authorization server to mint tokens the attacker replays against that resource.	8.0	More Details
CVE-2026-17333	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote attacker to bypass authentication and inject unauthorized configuration changes due to improper certificate validation.	8.0	More Details
CVE-2026-120408	The All-in-One Video Gallery WordPress plugin before 5.1.0 does not escape a video's stored thumbnail URL before outputting it in the admin video list, and does not sanitise that value when it is written outside its own editor, allowing users with a role as low as Subscriber to perform Stored Cross-Site Scripting attacks against administrators.	8.0	More Details
CVE-2026-96453	A flaw was found in the Keycloak Admin CLI kcadm tool, which is used by administrators to manage Keycloak servers from the command line. When a custom truststore is provided to verify the server identity, the tool incorrectly accepts any self-signed certificate as long as the hostname matches. This allows a network attacker to impersonate the Keycloak server, steal administrative credentials, and perform unauthorized management actions.	8.0	More Details

CVE-2026-17309	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote attacker to obtain sensitive information and tamper with configuration due to improper certificate validation.	8.0	More Details
CVE-2026-121139	The Rapid7 Metasploit msf-ws suffers from a missing authentication vulnerability whereby the REST API grants an unauthenticated "bootstrap" exemption so that the very first administrator can be created when the users table is empty. While the table is empty, POST /api/v1/users is exempt from authentication by design: the route handler calls warden.authenticate!(scope: :admin_api), which resolves to AdminApiToken. The inherited ApiToken#authenticate! short-circuits and returns success!() whenever msf.auth_initialized is false, without ever evaluating AdminApiToken's administrator check. In that state the endpoint creates a user — including an administrator — for an entirely unauthenticated caller. This issue has been fixed in version 6.5.9.	7.8	More Details
CVE-2026-59267	A crafted DXF document causes a heap buffer overflow in Draw in Apache OpenOffice 4.1.16 and earlier. This could cause a crash or otherwise a corruption of memory areas. Users are recommended to upgrade to version 4.1.17, which fixes this issue.	7.8	More Details
CVE-2026-123841	In JetBrains IntelliJ IDEA before 2026.3 code execution was possible via symlinks in an imported settings archive	7.8	More Details
CVE-2026-123837	In JetBrains IntelliJ IDEA before 2026.3, 2026.2.1 command injection was possible in untrusted projects via Tomcat run configurations on WSL	7.8	More Details
CVE-2026-121818	Herowatch Mini developed by About Time Technologies has a system signing vulnerability. Authenticated local attackers can exploit a publicly available test key to sign malicious programs, allowing them to elevate privileges and execute arbitrary code.	7.8	More Details
CVE-2026-87041	The RTIO submission-queue verifier rtio_vrfy_sqe() in subsys/rtio/rtio_syscalls.c (subsys/rtio/rtio_handlers.c before v4.3.0) accumulated the results of K_SYSCALL_MEMORY() into its valid_sqe flag with &=. That macro returns nonzero on failure (it is built on K_SYSCALL_VERIFY_MSG(), which yields !(expr)), so every buffer permission check contributed the opposite of its result. A submission whose tx.buf, rx.buf or txrx.tx_buf/txrx.rx_buf pointer was not accessible to the calling thread was accepted, while a legitimate, thread-owned buffer caused the calling thread to be killed with a kernel oops. The verifier runs on behalf of the rtio_sqe_copy_in_get_handles() system call (also reached through the inline rtio_sqe_copy_in() wrapper), so it is driven directly by untrusted user-mode input on any image built with CONFIG_USERSPACE. A user thread that has been granted an RTIO context and an rtio_iodev object — the intended usage of RTIO userspace support, established via rtio_access_grant() — can submit an SQE whose buffer pointer and length name arbitrary kernel memory; the object check on sqe->iodev is unaffected and still passes, and the crafted SQE is forwarded to the bus driver unchanged. Downstream consumers dereference the pointer with supervisor privilege. The generic I2C and I3C RTIO fallback handlers (drivers/i2c/i2c_rtio_default.c, drivers/i3c/i3c_rtio_default.c) copy sqe.rx.buf/sqe.tx.buf into struct i2c_msg and call i2c_transfer(), and the vendor SPI/I2C RTIO drivers behave equivalently. An RTIO_OP_RX submission therefore has peripheral data written into kernel memory of the attacker's choosing (arbitrary kernel write), an RTIO_OP_TX submission clocks kernel memory out over the bus (kernel memory disclosure), and a pointer to unmapped memory faults the kernel. This is a full escape from the user-mode isolation boundary that CONFIG_USERSPACE exists to enforce. The defect was masked for years because the in-tree user-mode RTIO tests only exercise RTIO_OP_NOP and mempool-backed reads, neither of which reaches the affected checks. The fix negates each K_SYSCALL_MEMORY() result and additionally validates the TXRX transmit buffer read-only, matching the SPI, I2C and I3C handlers.	7.8	More Details
CVE-2026-123974	In all versions of PyTorch's TorchServe, a predictable extraction directory in /tmp lets a local user swap the model handler and run code as the TorchServe service account leading to local privilege escalation.	7.8	More Details
CVE-2026-123853	In JetBrains IntelliJ IDEA before 2026.3, 2026.2.2 code execution was possible in Safe Mode via project-controlled JVM options of the build process	7.8	More Details
CVE-2026-87039	The user-mode syscall verifier z_vrfy_i2s_configure() in drivers/i2s/i2s_handlers.c copies the caller's struct i2s_config in from user memory and then, when cfg->frame_clk_freq is 0 (the API's "unconfigure the stream" request), jumps straight to z_impl_i2s_configure() without performing the K_SYSCALL_OBJ(config.mem_slab, K_OBJ_MEM_SLAB) ownership/type check or the block_size sanity check. The mem_slab field is a struct k_mem_slab *, so on that path a completely unvalidated, user-chosen pointer reaches driver code that is entitled to trust it as a real kernel object. Any thread running under CONFIG_USERSPACE that has access to an I2S device object can trigger this with a single i2s_configure() call. Most in-tree drivers special-case frame_clk_freq == 0 and never store the caller's structure, but drivers/i2s/i2s_litex.c does not: i2s_litex_configure() only logs a warning for a mismatched frame clock, then memcpy()s the caller's config into stream->cfg and marks the stream I2S_STATE_READY. A subsequent i2s_trigger() with I2S_TRIGGER_START enables the FIFO interrupt, and the interrupt handlers i2s_litex_isr_rx() / i2s_litex_isr_tx() then call k_mem_slab_alloc() and k_mem_slab_free() on the attacker-supplied pointer in supervisor context. The result is an arbitrary-pointer read/write primitive executed by the kernel on behalf of an unprivileged thread — k_mem_slab_alloc() takes a spinlock at slab->lock and reads and writes slab->free_list and the link word inside the returned "block" — which defeats the CONFIG_USERSPACE isolation boundary entirely. The same missing validation is a hazard for out-of-tree I2S drivers that retain the configuration on the unconfigure path. Builds without CONFIG_USERSPACE are unaffected, since the verifier is not	7.8	More Details

	used. The fix zeroes config.mem_slab and config.block_size on the unconfigure path so the driver can never receive an unvalidated pointer, while still allowing a stream to be unconfigured by a caller that does not own a memory slab, as the API documents.		
CVE-2026-123276	In JetBrains CLion before 2026.3, 2026.2.4.1 code execution was possible in Safe Mode via a crafted GDB server debug profile	7.8	More Details
CVE-2026-120859	PyMoDAQ before 4.4.13, and pymodaq_data, pymodaq_gui, and pymodaq_utils before 5.1.15, 5.2.x before 5.2.14, and 5.3.x before 5.3.10, contain deserialization of untrusted data and eval injection vulnerabilities that allow attackers to execute arbitrary code by supplying crafted files that a user opens. Attackers can store pickled objects in HDF5 string nodes that StringARRAY.array_to_string() passes to pickle.loads() when the node is browsed or read, place Python expressions in HDF5 attributes that JsonConverter.json2object() evaluates, supply a .dock file that load_layout_state() unpickles from the Dashboard Load layout action, or embed Python expressions in XML settings files that elt_to_dict() and set_txt_from_elt() evaluate.	7.8	More Details
CVE-2026-123838	In JetBrains IntelliJ IDEA before 2026.3 code execution was possible in Safe Mode via UI Designer form file	7.8	More Details
CVE-2026-121941	libmt32emu before 2.8.4 contains a heap buffer overflow vulnerability in MidiStreamParserImpl::parseSysex that allows attackers to write past a heap allocation by supplying oversized unterminated SysEx messages. Attackers can feed more than 32768 SysEx data bytes through the mt32emu_parse_stream API via MIDI files, ports, or sequencer clients to corrupt heap memory and crash the application.	7.8	More Details
CVE-2026-122328	SDL_mixer 3.1.2 through 3.2.4 contains a stack-based buffer overflow vulnerability in FetchXLaw() of src/decoder_wav.c when decoding A-law or mu-law WAV files. Attackers can supply a crafted WAV file whose doubly-offset float expansion overwrites about 1 KB of adjacent stack memory, causing crashes or potentially code execution.	7.8	More Details
CVE-2026-123304	In JetBrains IntelliJ IDEA before 2026.3 code execution in untrusted projects via a configured ShellCheck path	7.8	More Details
CVE-2026-44875	In HPE Cray Programming Environment versions 25.03 and 25.09, prior to 26.03, the method that CPE is deployed on HPCM potentially allows elevated access by a local unprivileged user.	7.8	More Details
CVE-2026-100081	In the Linux kernel, the following vulnerability has been resolved: xen-netback: defer xenvif_mcast_addr_list_free() In order for the function to legitimately avoid locking/RCU, it needs to run after all TX/RX processing has finished/stopped: Lookups happen from xenvif_start_xmit(), while adds/removes happen from xenvif_tx_action() (called out of xenvif_poll()). Move the call out of xenvif_disconnect_data() (the call to the function from connect()'s error path doesn't require any cleaning up there), and put it past the synchronization point in backend_disconnect(). This is XSA-527 / CVE-2026-100081.	7.8	More Details
CVE-2026-59264	The Windows installers of Apache OpenOffice 4.1.16 and earlier allow an already manipulated system to run external code with elevated access. Users are recommended to upgrade to version 4.1.17, which fixes this issue.	7.8	More Details
CVE-2026-123321	In JetBrains WebStorm before 2026.3, 2026.2.3 code execution via Grunt and Gulp task loading was possible in untrusted projects	7.8	More Details
CVE-2026-120499	h5io before 0.2.6 contains a code injection vulnerability in read_hdf5() that allows attackers to execute arbitrary code by supplying a crafted HDF5 file. Attackers can store Python code in a node titled timezone, which _triage_read() passes to eval() with builtins reachable, name an arbitrary module in class or custom-object nodes that _import_class() imports, or place pickled objects in pd_dataframe or pd_series nodes that pandas deserializes on read.	7.8	More Details
CVE-2026-119083	Path traversal in the archive extraction utility in GluonTS before 0.17.0 might allow an actor who supplies a crafted tar archive to write arbitrary files outside the intended extraction directory with the privileges of the extracting process via symbolic or hard links contained in the archive. To remediate this issue, users should upgrade to version 0.17.0 or later.	7.8	More Details
CVE-2026-68990	In the Samsung Exynos H-Arx DRM plugin, improper input validation during buffer operations can cause memory corruption, potentially leading to denial of service or privilege escalation.	7.8	More Details
CVE-2026-123302	In JetBrains IntelliJ IDEA before 2026.3, 2026.2.4, 2026.1.5.1, 2025.3.6.2 code execution was possible in untrusted projects via script engine discovery	7.8	More Details
CVE-2026-123293	In JetBrains IntelliJ IDEA before 2026.3, 2026.2.4 code execution was possible in untrusted projects via the Terraform tool path setting	7.8	More Details

CVE-2026-123784	Fluxbox through 1.3.7 contains an OS command injection vulnerability in RootTheme::reconfigTheme() that allows attackers to execute commands via crafted style background values. Attackers can embed shell metacharacters in background pixmap paths, random directories, or gradient texture text, which are concatenated unescaped into an fbsetbg command run via $SHELL -c when the style loads.	7.8	More Details
CVE-2019-16447	Adobe Illustrator CC versions 23.1 and earlier have a binary planting vulnerability. Successful exploitation could lead to local code execution.	7.8	More Details
CVE-2026-102739	ESPectre is a Wi-Fi motion sensing platform for ESP32. Prior to 3.0.0-rc1, Micro-ESPectre analysis tools, including tools/6_optimize_filter_params.py, tools/1_analyze_raw_data.py, and tools/10_train_ml_model.py, load NPZ datasets with NumPy pickle support enabled through micro-espectre/tools/csi_utils.py and a direct loader. A malicious dataset contributor or pull-request author can place an object-typed array in a .npz file under micro-espectre/data, causing pickle-controlled code to execute as the maintainer or developer when a documented analysis tool accesses the field. This issue is fixed in version 3.0.0-rc1.	7.8	More Details
CVE-2026-70659	stable-diffusion.cpp is a pure C/C++ library for running diffusion model (Stable Diffusion, Flux, Wan, Qwen Image, Z-Image, and more) inference. From master-742-1a13107 until master-763-4fcc6fe, IMatrixCollector::load_imatrix in src/runtime/imatrix.cpp reuses the values and counts vectors for entries with the same tensor name but resizes them only when they are empty. An untrusted .imatrix file can provide a small nval for the first entry and a larger nval for a second entry with the same name, causing the accumulation loop to write attacker-controlled floating-point and integer values beyond both heap buffers. Loading the file through the --imat-in conversion path can corrupt the heap or crash the process before a model is required. This issue is fixed in master-763-4fcc6fe.	7.8	More Details
CVE-2026-90975	A vulnerability in Realtek's RtUsbA64.sys USB audio driver allows a local, low-privileged user to abuse a kernel I/O control (IOCTL) interface that acts on a caller-supplied user-mode pointer without proper validation or capture. By issuing crafted property requests an attacker can obtain kernel-mode read and write access, which can be leveraged for local privilege escalation and arbitrary kernel code execution.	7.8	More Details
CVE-2026-122329	SDL_mixer 3.1.2 through 3.2.4 contains a stack-based buffer overflow in FetchXLaw() in src/decoder_aiff.c due to miscalculated output offsets when expanding A-law or mu-law samples. Attackers can supply a crafted AIFF-C file that overwrites roughly 1 KB of adjacent stack memory when decoded, causing crashes or potential code execution.	7.8	More Details
CVE-2026-122307	Kyverno before 1.19.2 contains a policy bypass vulnerability in the admissionpolicygenerator controller, which folds PolicyExceptions into generated ValidatingAdmissionPolicies while ignoring the --enablePolicyException, --exceptionNamespace, and policy kind gates. Users with namespaced create rights on PolicyExceptions can inject negated matchConditions into the generated policies to admit violating resources, bypassing cluster-wide enforcement.	7.7	More Details
CVE-2026-17345	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to improper neutralization of special elements used in an SQL command.	7.7	More Details
CVE-2026-107912	A flaw was found in the management interface of the Quarkus framework, specifically within the quarkus-vertx-http component. The issue occurs when the framework incorrectly combines the management root path with specific permission rules, leading to a situation where security policies are applied to the wrong internal paths. As a result, an attacker can bypass intended authorization checks and gain unauthorized access to sensitive management endpoints.	7.7	More Details
CVE-2026-122305	Kyverno before 1.19.2 contains a denial of service vulnerability in substituteVariablesIfAny that allows low-privileged users to hang the admission webhook via self-referential variable templates. Attackers can create resources whose annotations re-introduce the embedded policy variable, causing unbounded substitution loops that exhaust CPU and memory and block cluster-wide admission.	7.7	More Details
CVE-2026-123324	In JetBrains YouTrack before 2026.2.19562 information disclosure via shared mailbox message history was possible	7.7	More Details
CVE-2026-122318	Kyverno before 1.19.2 contains an authentication bypass in matchCertificateData that skips verifyImages subject and subjectRegExp checks when the signing certificate has no Subject Alternative Name. Attackers holding a leaf certificate from a configured private trust root can omit the SAN, set the expected Fulcio issuer OID, and sign malicious images that are admitted despite signer pinning.	7.7	More Details
CVE-2026-122312	Kyverno from 1.19.1 before 1.19.2 contains a namespace isolation bypass in APICall Fetch() in pkg/engine/apicall/apiCall.go because path.Clean treats '?' as a path character, letting the namespace regex match segments inside the query string. Users who can create namespaced policies can supply a URLPath like /api/v1/nodes?x=/namespaces/default/ that passes validation while client-go requests the cluster-scoped endpoint, reading resources outside their namespace.	7.7	More Details
CVE-2026-17375	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to improper authorization. Authorization decisions rely on information supplied by the client, which could allow access to information the user should not see.	7.7	More Details

CVE-2026-17361	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to server-side request forgery.	7.7	More Details
CVE-2026-17363	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to SQL injection.	7.7	More Details
CVE-2026-17373	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to improper authorization.	7.7	More Details
CVE-2026-17374	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to broken object-level authorization.	7.7	More Details
CVE-2026-17376	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to broken object-level authorization.	7.7	More Details
CVE-2026-54382	VitaFit cloud API before 2026-10-30 contained an improper access control vulnerability in its Cognito-issued AWS role that allows authenticated attackers to perform s3:PutObject operations across the entire shared bucket instead of being restricted to their own folder. Attackers can overwrite other users' objects in the shared S3 bucket using credentials obtained via CVE-2026-54378, destroying original content without triggering deletion protections.	7.7	More Details
CVE-2026-122320	Kyverno before 1.19.2 contains a missing authorization vulnerability that allows namespaced Policy authors to read resources in other namespaces by templating generate.clone or cloneList namespace values. Attackers can annotate a triggering ConfigMap so the background-controller copies a victim namespace's sensitive ConfigMap into the attacker's namespace, enabling cross-tenant data disclosure.	7.7	More Details
CVE-2026-17378	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to broken object-level authorization.	7.7	More Details
CVE-2026-17383	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information from other tenants due to broken object-level authorization.	7.7	More Details
CVE-2026-17387	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to broken object-level authorization.	7.7	More Details
CVE-2026-17400	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to SQL injection.	7.7	More Details
CVE-2026-77779	ManageEngine Key Manager Plus versions before 7151 were vulnerable to an Improper Access Control vulnerability that allowed authenticated low-privilege users to export keys outside their authorized scope.	7.7	More Details
CVE-2026-122306	Kyverno before 1.19.2 contains a denial of service vulnerability that allows namespaced policy authors to exhaust admission controller CPU by submitting pathological wildcard patterns. Attackers can create a Policy with crafted match and exclude names evaluated by ValidateMatchExcludeConflict, pinning cores and causing cluster-wide webhook timeouts that block resource operations.	7.7	More Details
CVE-2026-17320	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to an insecure direct object reference.	7.7	More Details
CVE-2026-17279	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to cause a denial of service due to uncontrolled resource consumption. Certain requests can cause internal processing to stall, which could make the service unavailable.	7.7	More Details
CVE-2026-49407	OpenHuman is an open-source agent harness available as a desktop application and Rust library. Before version 0.57.44, its local /ws/dictation WebSocket endpoint lacks client authentication and browser-origin validation. An unauthenticated client, including a malicious web page able to reach the endpoint, can submit audio and trigger resource-intensive speech-to-text processing. Earlier affected versions also accumulate audio in an unbounded buffer, allowing continuous streaming to exhaust process memory. These conditions can degrade performance, exhaust resources, or crash the application. This issue is fixed in version 0.57.44.	7.7	More Details
CVE-2026-16712	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information from other tenants due to improper authorization. Identifiers supplied in requests are not sufficiently checked against the user's permissions, which could allow access to data belonging to other tenants.	7.7	More Details

CVE-2026-16715	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information from other tenants due to broken object-level authorization.	7.7	More Details
CVE-2026-16717	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to broken object-level authorization.	7.7	More Details
CVE-2026-16718	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to improper validation of file paths.	7.7	More Details
CVE-2026-16854	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information belonging to other tenants due to an injection vulnerability. Input used to build a data query is not properly neutralized, which could allow the query to return data the user is not permitted to see.	7.7	More Details
CVE-2026-111770	The Model Context Protocol TypeScript SDK provides TypeScript client and server implementations of the Model Context Protocol. From 2.0.0 until 2.3.0 in @modelcontextprotocol/server, applications that shared one stateless HTTP transport or one McpServer or Server instance among multiple clients could deliver responses and notifications to the wrong client. The affected surface is an MCP server reached over HTTP by multiple clients. The trigger is reuse of one stateless transport or server instance. Messages were associated with a connection using only the JSON-RPC request identifier. SDK clients start request identifiers at zero, so collisions occur in normal operation. Cross-client delivery exposes one client's responses and notifications to another client. The issue requires an HTTP endpoint reachable by more than one client and an application that constructs the server or transport once at startup instead of once per request or session. stdio servers and factory-created per-call servers are not affected. Upgrading causes reused instances to fail and therefore requires an application code change. This issue is fixed in @modelcontextprotocol/server 2.3.0.	7.7	More Details
CVE-2026-17112	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information belonging to other tenants due to broken object-level authorization.	7.7	More Details
CVE-2026-119431	A server-side request forgery (SSRF) vulnerability exists in Foxit Workspace's file-upload functionality. Insufficient validation of user-supplied links may allow a remote attacker to induce the server to access internal resources and return their contents, potentially resulting in sensitive information disclosure and unauthorized access to internal services.	7.7	More Details
CVE-2026-119433	A server-side request forgery (SSRF) vulnerability exists in an undocumented API endpoint of Foxit Workspace due to insufficient validation of user-supplied URL and network parameters. A remote attacker could exploit this issue to induce the server to send requests to arbitrary internal or external resources, potentially enabling unauthorized access to internal services, network reconnaissance, and sensitive information disclosure.	7.7	More Details
CVE-2026-61649	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to 7.15.2 and 8.10.2, the SSRF protection added in 7.15.1 uses a substring comparison in isSelfRequest() rather than hostname equality. The affected flow begins at validate_external_host() and uses isSelfRequest(), and stripos() to carry attacker-controlled data or authorization state into the security-sensitive operation. An authenticated attacker can place the server hostname in a URL path to bypass IP validation and direct server-side requests to internal services. This issue is fixed in versions 7.15.2 and 8.10.2.	7.7	More Details
CVE-2026-17318	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to improper authorization.	7.7	More Details
CVE-2026-17282	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to broken object-level authorization.	7.7	More Details
CVE-2026-17289	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to server-side request forgery.	7.7	More Details
CVE-2026-69137	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to 7.15.2 and 8.10.2, the CalendarAccount testConnection action passes an authenticated caller's server_url directly to curl without host, address, or scheme validation. The affected flow begins at CalendarAccount::action_testConnection and uses server_url, CalDAVProvider::makeCalDAVRequest(), and PROPFIND to carry attacker-controlled data or authorization state into the security-sensitive operation. The server sends a PROPFIND request from its network context and returns non-success response bodies, enabling internal-service access, partial response disclosure, service enumeration, and possible cloud metadata access. This issue is fixed in versions 7.15.2 and 8.10.2.	7.7	More Details
CVE-2026-17281	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to server-side request forgery.	7.7	More Details

CVE-2026-62856	FreeScout is a self-hosted help desk and shared mailbox application. Prior to version 1.8.226, the polycast/receive endpoint fails to escape SQL LIKE wildcards in supplied channel names, while channel authorization applies only to names with specific prefixes. An unauthenticated attacker with a guest session and valid CSRF token can submit a wildcard channel name to retrieve matching notification events intended for other users. Notification payload generation lacks a corresponding access check, exposing conversation message content, identifiers, URLs, and notification HTML across users and mailboxes. This issue is fixed in version 1.8.226.	7.7	More Details
CVE-2026-17285	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to improper validation of external references. When schemas are validated, references to external resources are not sufficiently restricted, which could allow the server to retrieve content it should not access.	7.7	More Details
CVE-2026-17283	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to broken object-level authorization.	7.7	More Details
CVE-2026-17295	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to path traversal.	7.7	More Details
CVE-2026-17411	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow an authenticated attacker to view, add, modify, or delete information in the back-end database due to SQL injection. Input is not properly neutralized before it is used in database queries.	7.6	More Details
CVE-2026-121945	CoopCycle coopcycle-web before 6.20.1 contains a broken access control vulnerability that allows any courier to read and modify every incident because Incident operations only check ROLE_COURIER. Attackers can enumerate sequential incident ids and use PUT /api/incidents/{id}/action to re-price, cancel or reschedule other stores' orders and tasks.	7.6	More Details
CVE-2026-62854	FreeScout is a self-hosted help desk and shared mailbox. Prior to 1.8.225, a user who can edit a mailbox signature can combine a scriptable file uploaded through /uploads/upload with nested tag fragments that bypass Helper::stripDangerousTags(). The resulting external script is served from the same origin, so the script-src 'self' policy permits it when another user opens the affected mailbox reply editor or new-ticket page. The script executes with the victim's FreeScout privileges and can read visible data and perform same-origin actions. This issue is fixed in version 1.8.225.	7.6	More Details
CVE-2026-102615	HeyForm is an open-source form builder. Prior to 3.0.1, /api/upload accepts a file according to the client-controlled multipart file.mimetype while retaining an HTML filename, and static/upload serves the resulting file as text/html with contentSecurityPolicy: false. An ordinary user can therefore upload active HTML that executes on the HeyForm origin when a victim opens its returned URL. The same-origin script can access /graphql with the victim's session and read or modify data available to that account. The code also permits upload requests tied to an active public form through formId, openToken, and a fieldId belonging to a file or signature question, although the advisory did not fully verify that unauthenticated path end to end. This issue is fixed in version 3.0.1.	7.6	More Details
CVE-2026-17357	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to access internal network services due to server-side request forgery.	7.6	More Details
CVE-2026-58141	Dify before 1.15.0 contains a server-side request forgery vulnerability that allows any authenticated console user to bypass SSRF protections and issue arbitrary HTTP requests to internal services and cloud metadata endpoints due to the Squid proxy configuration only defining source ACLs without destination deny rules and the make_request() helper performing no independent destination IP validation. Attackers can use endpoints such as GET /console/api/remote-files/<url>, POST /console/api/remote-files/upload, the HTTP Request workflow node, website crawl, or document import from URL to reach internal components like the sandbox, internal APIs, and PostgreSQL, and on AWS deployments read IAM credentials from the instance metadata service, with the HTTP Request node further enabling POST, PUT, and DELETE writes to internal services relying on network isolation for authorization.	7.6	More Details
CVE-2026-103479	The Pubjet | پابجت plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 5.4.8. This is due to the `checkToken()` AJAX handler — registered under `wp_ajax_pubjet-check-token` — performing no capability check and no nonce verification before unconditionally writing the attacker-supplied `token` GET parameter directly into the site-wide `pubjet_settings` option via `pubjet_update_setting()`, prior to any remote validation. This makes it possible for authenticated attackers, with Subscriber-level access and above, to overwrite the plugin's stored REST API credential with an attacker-chosen value, immediately elevating their effective privileges to those of an authorized Pubjet API client and enabling them to invoke otherwise-restricted endpoints — `createReportage`, `updateReportage`, `deleteReportage`, `toggleCopyright`, and `createBacklink` — to create, modify, and delete arbitrary reportage posts and manipulate plugin state that Subscribers cannot normally access. The privilege escalation is self-reinforcing: because `RestApi::isTokenValid()` authenticates solely by comparing the incoming `Authorization` header against the value returned by `pubjet_token()`, which reads from the same option the unprotected handler writes to, the attacker-planted token is trusted as legitimate on all subsequent requests.	7.6	More Details
	Wanderer is a self-hosted trail database for saving and sharing adventures. Prior to 0.19.3, an authenticated local user can submit crafted waypoint.name and waypoint.icon values that the trail elevation graph interpolates into		

CVE-2026-62346	an innerHTML template in web/src/lib/vendor/maplibre-elevation-profile/elevationprofile.ts without HTML encoding or icon validation. A victim viewing the elevation profile executes the attacker-controlled script in their browser. Separately, federated waypoints can deliver the same malicious fields across instances without requiring the attacker to have a local account on the receiving instance. The script can expose session data or perform actions in the victim's context. This issue is fixed in version 0.19.3.	7.6	More Details
CVE-2026-62345	Wanderer is a self-hosted trail database for saving and sharing adventures. Prior to 0.19.3, an authenticated user can store a crafted waypoint.icon value that createMarkerFromWaypoint() passes into FontawesomeMarker, where insertAdjacentHTML inserts the unvalidated value into map marker markup. Opening the affected trail map executes attacker-controlled script in the viewer's browser, which can expose session tokens or perform actions as the victim. Federated waypoint data can also reach the sink without a local account on the receiving instance. This issue is fixed in version 0.19.3.	7.6	More Details
CVE-2026-76506	A vulnerability in the web-based management interface of Cisco UCS Central Software could allow an authenticated, remote attacker to achieve remote code execution or conduct information disclosure attacks on an affected device. This vulnerability is due to insufficient validation of user-supplied input in an HTTP request. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected endpoint on an affected device. A successful exploit could allow the attacker to execute arbitrary commands, write arbitrary files to the filesystem, and obtain sensitive information. To exploit this vulnerability, the attacker must have valid user credentials on the affected device. Cisco has released software updates that address this vulnerability There are no workarounds that address this vulnerability.	7.6	More Details
CVE-2026-80335	Memory Corruption when processing firmware update data in Download mode due to a missing bounds check.	7.6	More Details
CVE-2026-17129	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information and cause a denial of service due to an insecure direct object reference.	7.6	More Details
CVE-2026-105413	The Form Maker by 10Web WordPress plugin before 1.15.51 does not consistently escape user-submitted field values before rendering them on its submissions admin page, allowing unauthenticated users to store a payload that executes as arbitrary web scripts in the session of an administrator who views the submissions.	7.5	More Details
CVE-2026-104010	The WPSyncSheets For Contact Form 7 – CF7 Google Sheets Connector & Save to Database plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 1.8.0 via the 'any non-system CF7 field (e.g., your-message)' parameter parameter. This is due to insufficient sanitization of CF7 submission field values before database storage and the absence of an allowed_classes restriction on maybe_unserialize() during admin retrieval. This makes it possible for unauthenticated attackers to execute code on the server. Successful exploitation of the remote code execution gadget chain requires that a Google Sheets access token be configured in the plugin (its primary advertised feature), as this triggers autoloading of the bundled Monolog 2.10.0 library whose classes form the exploitable gadget chain; however, the underlying PHP Object Injection occurs regardless.	7.5	More Details
CVE-2026-123047	In Eclipse BaSyx Helm Charts versions 3.0.0-rc.1 to 3.12.1 of the `basyx` chart, deployments with the bundled Keycloak enabled store the passwords of the Keycloak users that the chart creates in cleartext in a Kubernetes ConfigMap. The template `keycloak-init-config.yaml` rendered `keycloak.initialization.users`, including each user's `credentials[].value`, as `users.json` into the persistent ConfigMap `<release>-basyx-keycloak-init-config`. By default this includes the bootstrap administrator user. That user holds the `admin` role and has a non-temporary password. A principal that can read ConfigMaps but not Secrets in the release namespace, such as a holder of the built-in Kubernetes `view` ClusterRole, can read the password from the ConfigMap and log in to Keycloak as this user. The resulting token carries the `admin` role, which the default BaSyx ABAC rules map to full rights on all BaSyx APIs in the deployment. The bundled Keycloak is disabled by default. The issue is fixed in version 3.12.2 of the `basyx` chart, which moves the initialization users to the Keycloak credentials Secret. Affected users should upgrade and change the passwords of users that were created through the chart.	7.5	More Details
CVE-2026-103866	Inconsistent interpretation of HTTP requests ('HTTP Request/Response smuggling') vulnerability in Apache Sling Engine. The engine's query/form parser accepts non-standard percent-escapes, wrong charsets, and continues request processing on such errors. This issue affects Apache Sling Engine: before 3.0.4. Users are recommended to upgrade to version 3.0.4, which fixes the issue.	7.5	More Details
CVE-2026-103864	Improper output neutralization for logs in Apache Sling Engine. This issue affects Apache Sling Engine: before 3.0.4. Users are recommended to upgrade to version 3.0.4, which fixes the issue.	7.5	More Details
CVE-2026-116567	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to 1.11.2, rtmp_handle_control() rendered an RTMP user-control message into a 200-byte stack buffer using an unbounded sprintf loop controlled by the wire message length. A body of roughly 70 bytes or more overflowed the stack before any RTMP login, because the handshake authenticates neither side. The flaw affects deployments that build and load mod_rtmp, which is disabled in the stock build and configuration but commonly exposes a listener on TCP port 1935 when enabled. One unauthenticated message can crash FreeSWITCH and end every active call; the constrained ASCII hex output has not yielded control-flow hijacking. This issue is fixed in version 1.11.2.	7.5	More Details
	Chartbrew is an open-source web application that can connect directly to databases and APIs and use the data to		

CVE-2026-68933	create charts. Prior to 5.2.3, public dashboard passwords were stored in plaintext, accepted through a URL query parameter, and checked without effective attempt throttling. The vulnerable surface is public password-protected dashboard storage and validation routes. An unauthenticated attacker targets a public password-protected dashboard and repeatedly submits candidate passwords or obtains password-bearing server or proxy logs. Unlimited online guesses enable brute force, while cleartext storage and URL transport expose the secret in application storage and server or proxy access logs. The target must be a public dashboard with password protection enabled. Even failed attempts reveal chart count and configuration without the password; a recovered password grants access to the protected dashboard and its chart data. This vulnerability is fixed in 5.2.3.	7.5	More Details
CVE-2026-107616	The Amelia plugin for WordPress is vulnerable to unauthorized access of attendee data due to a missing authorization check on the GetEventAttendeesCommandHandler::handle() function in versions up to, and including, 9.9.1. The handler only enforces the broad `amelia_read_events` capability — which the plugin's own `wpamelia-customer` role possesses — and does not verify that the authenticated user is an organizer/provider of the event referenced by the client-supplied `id` query parameter. This makes it possible for authenticated attackers, with wpamelia-customer-level access and above, to export the full CSV of attendee personally identifiable information (first/last name, email, phone, date of birth, gender, private notes, payment amounts/methods, WooCommerce order IDs, custom-field values, and uploaded-file URLs) for any Amelia event on the site by directly invoking the `/report/event/attendees` endpoint with an arbitrary event ID.	7.5	More Details
CVE-2026-123327	In JetBrains YouTrack before 2026.2.19562 missing authorization in the saved query endpoint allowed disclosure of issue descriptions	7.5	More Details
CVE-2026-119164	The wpForo Forum plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 3.2.2 via the `data[secondary_groupids]` parameter of the `wpforo_action_profile_update` POST handler. This is due to a type-confusion flaw in the secondary_groupids authorization guard within the `Members::update()` function in `classes/Members.php`, where casting a scalar CSV string (e.g. `"0,1"`) with `(array)` before `array_map('intval', ...)` and `array_filter()` produces an empty array — causing the guard's outer conditional, and the else-branch that would otherwise strip the field from the update, to be bypassed entirely — while `encode()`/`decode()` downstream correctly explodes the original CSV and persists the attacker-supplied group IDs to `wp_wpforo_profiles.secondary_groupids`. This makes it possible for authenticated attackers, with Subscriber-level access and above, to escalate their forum privileges to wpForo Administrator by injecting the privileged Admin group ID, granting access to the Forum Accesses editor and the ability to rewrite forum-wide capability policies for all members and edit arbitrary content owned by other users. Exploitation requires the attacker to have at least 3 approved wpForo posts to satisfy the plugin's default `min_number_posts_to_edit_account` antispam gate, along with a valid wpforo nonce obtained from their own account profile form.	7.5	More Details
CVE-2026-116568	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to 1.11.2, rtmp_rtmp2rtpH264() trusted the length prefix of each inbound H.264 NAL unit without checking it against the bytes remaining in the RTMP message. An oversized declared unit underflowed the unsigned remaining-byte counter and advanced the parser beyond its receive buffer, where the next length-prefix read could crash the process. The flaw affects deployments that build and load mod_rtmp and accept video call sessions, commonly on TCP port 1935; placing the call requires a directory login where auth-calls is true, while no credentials are required where auth-calls is absent or false. A remote client can terminate FreeSWITCH and every active call, but the defect supplies no write primitive and memory disclosure has not been demonstrated. This issue is fixed in version 1.11.2.	7.5	More Details
CVE-2026-119155	The wpForo Forum plugin for WordPress is vulnerable to time-based SQL Injection via the 'href[locale]' parameter in all versions up to, and including, 3.2.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. The nonce required for exploitation is publicly issued to unauthenticated visitors on any forum page via the wpforo.nonces JavaScript object, meaning no account or prior interaction beyond a page load is required to obtain it.	7.5	More Details
CVE-2026-120651	CGI versions before 5.00 for Perl allow an infinite loop on a short request body when $DISABLE_UPLOADS is set. When $CGI::PUTDATA_UPLOAD or an upload hook is set, read_postdata_putdata takes a request body that is not a form submission. With $CGI::DISABLE_UPLOADS set, it discards the body by reading until Content-Length bytes have arrived. Once a body shorter than its Content-Length runs out, every read returns 0, so the loop never ends. A client can keep a server process spinning with one such request.	7.5	More Details
CVE-2026-123029	Wowza Streaming Engine before 4.12.2 processes XML external entities, which allows remote attackers to read local files with the privileges of the Wowza Streaming Engine process.	7.5	More Details
CVE-2026-116569	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to 1.11.2, msrp_parse_buffer() subtracted delimiter framing from a peer-controlled short segment whose MSRP byte range ended in * without first proving the segment was long enough. The unsigned result wrapped near SIZE_MAX and reached switch_msrp_msg_set_payload() as both an allocation size and memcpy length, while related pointer arithmetic could read before the receive buffer. The listener is disabled by default in msrp.conf.xml, but any deployment enabling an MSRP TCP or TLS port parses this framing before authentication. An unauthenticated	7.5	More Details

	network peer can corrupt memory and crash FreeSWITCH, dropping all active calls, although remote code execution has not been demonstrated. This issue is fixed in version 1.11.2.		
CVE-2026-116570	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to 1.11.2, http_directory_auth() rebuilt an expected user@domain:password credential and base64-encoded it into an 80-byte buffer using an encoder without an output-length argument. A configured credential longer than 57 characters overflowed the stack before the supplied HTTP Basic password was compared. An unauthenticated client only needed to name an existing directory user on an exposed mod_xml_rpc HTTP listener; the module is built but not loaded by the stock configuration. The overflow can corrupt the stack and crash FreeSWITCH, ending every active call, although the overrun bytes come from the configured credential and remote code execution has not been demonstrated. This issue is fixed in version 1.11.2.	7.5	More Details
CVE-2026-115928	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to 1.11.2, switch_core_media_add_crypto() passed the encoded key and salt length from an inbound SDP a=crypto attribute to switch_b64_decode() as the destination capacity. A zero-length key and salt made that capacity underflow, allowing the decoded attribute to overflow a fixed stack buffer with sender-chosen bytes before the call was answered. On the shipped external profile, an unauthenticated caller can reach the SDES-SRTP parser, while profiles that challenge inbound calls remain affected for senders who can authenticate; setting rtp_secure_media_inbound to false removes the path, and WebRTC DTLS-SRTP legs are unaffected. The overflow corrupts memory and can crash the FreeSWITCH process, dropping every active call, although remote code execution has not been demonstrated. This issue is fixed in version 1.11.2.	7.5	More Details
CVE-2026-121617	A security flaw has been discovered in Linksys E5600 1.1.0.26. Affected by this issue is the function init_multipart of the file /cgi-bin/upload_fw.cgi of the component Header Parser. The manipulation results in out-of-bounds write. The attack may be launched 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. This vulnerability only affects products that are no longer supported by the maintainer.	7.5	More Details
CVE-2026-123655	A flaw was found in Moodle. Insufficient access control checks on H5P content files allow unauthenticated remote attackers to view restricted materials, including content stored in the system context and files belonging to hidden or unavailable course modules. This issue results in unauthorized information disclosure of protected content.	7.5	More Details
CVE-2026-49939	In Apache James server prior version 3.9.1 improper Access Control List processing is exposed by the JMAP protocol which do not account for negative rules positionned by IMAP protocol. This results in users being able to administer folders in JMAP despite having being explicitly denied the right to do so in IMAP. Users are recommended to upgrade to version 3.9.1 which fixes this issue.	7.5	More Details
CVE-2026-122314	Kyverno before 1.19.2 contains an unchecked type assertion in its variable-substitution engine that allows users who can submit resources to crash the policy engine. Attackers can submit resources with non-string fields referenced by {{- variable }} shallow substitution in policies, causing a panic that yields webhook denial of service and policy bypass under failurePolicy Ignore.	7.5	More Details
CVE-2026-122315	Kyverno before 1.19.2 contains an unchecked type assertion in buildStatementMap that allows unauthenticated attackers to crash the policy engine via crafted attestation statements. Attackers can push an OCI referrer manifest with a non-string type field to bypass image verification under failurePolicy Ignore or crash-loop the reports-controller.	7.5	More Details
CVE-2026-79405	Transient DOS when processing a malformed NR RRC configuration message due to improper input validation.	7.5	More Details
CVE-2026-122319	Kyverno before 1.19.2 contains a denial-of-service vulnerability in the In and NotIn operators that allows attackers to crash the policy engine via an unchecked type assertion. Attackers can submit resources whose JMESPath-evaluated values yield arrays of integers, booleans, or mixed types, triggering a panic that disrupts admission control and policy enforcement.	7.5	More Details
CVE-2026-122322	Kyverno from 1.11.0 before 1.19.2 contains an unbounded decompression vulnerability in extractStatement that allows remote attackers to exhaust memory by supplying highly compressed attestation layers. Attackers controlling registry referrer artifacts can push gzip predicate layers exceeding maxPayloadSize when decompressed, causing admission controller OOM kills and denial of service.	7.5	More Details
CVE-2026-122323	Kyverno from 1.11.0 before 1.19.2 contains an unbounded decompression vulnerability in FetchSignatureBlob that allows attackers to exhaust memory by supplying highly compressed notary signature layers. Attackers who control registry referrers or signatures can publish small gzip layers that decompress beyond maxPayloadSize, causing admission controller OOM kills and denial of service.	7.5	More Details
CVE-2026-33958	Processing a malformed RRC Reconfiguration message leads to an out-of-bounds (OOB) access, resulting in a denial-of-service (DoS) condition.	7.5	More Details
CVE-	In the NAS Authentication Request message decoding procedure, a missing lower bound check causes an infinite		More

2026-33969	loop, leading to Denial of Service.	7.5	Details
CVE-2026-35494	In the baseband, memory corruption during NAS packet processing can cause a denial of service.	7.5	More Details
CVE-2026-48176	A memory corruption vulnerability caused by improper validation of messages	7.5	More Details
CVE-2026-48179	In the Exynos modem's IMS stack, improper handling of SDP payload leads to a Denial of Service	7.5	More Details
CVE-2026-104720	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Kobikom Telecommunications and Informatics Services Inc. Kobikom allows Path Traversal. This issue affects Kobikom: before KobiPBX-FOP3-SEC-r1.	7.5	More Details
CVE-2026-68985	In the Samsung Exynos NPU driver, improper validation of user input in the ioctl handler can lead to an out-of-bounds write, which causes a denial of service.	7.5	More Details
CVE-2026-123202	libnxml before 0.18.6 contains a stack-based buffer overflow vulnerability in src/nxml_parser.c that allows remote attackers to write past a 1024-byte stack buffer via long XML names. Attackers can supply XML or RSS feeds with a 1022-character element, attribute, DOCTYPE or entity name ending in a multi-byte UTF-8 character to crash parsing applications.	7.5	More Details
CVE-2026-69002	Incorrect authorization in Samsung framework services due to missing permission checks	7.5	More Details
CVE-2026-69025	In the Exynos NPU driver, improper validation of user input in the ioctl handler can lead to an out-of-bounds write, which causes a denial of service	7.5	More Details
CVE-2026-116751	The Booking for Appointments and Events Calendar – Amelia Pro plugin for WordPress is vulnerable to time-based SQL Injection via the 'tag[] (array KEYS)' parameter in all versions up to, and including, 9.9.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. WordPress's wp_magic_quotes escapes array values but not array keys, meaning attacker-controlled tag[] array keys reach EventRepository::getFilteredIds() completely unescaped and can be crafted to defeat the plugin's Statement::execute placeholder binder via overlapping strtr() substitution keys.	7.5	More Details
CVE-2026-123200	VRPN through 07.36 contains an out-of-bounds stack write vulnerability in vrpn_Endpoint::handle_sender_message() and handle_type_message() that allows unauthenticated remote peers to write outside a stack buffer via an unchecked length index. Attackers can connect, complete the version-cookie exchange, and send a SENDER_DESCRIPTION or TYPE_DESCRIPTION message with an out-of-range or negative index to crash the process.	7.5	More Details
CVE-2026-85108	Allocation of Resources Without Limits or Throttling in Apache James Mime4J library prior version 0.8.15 allows Denial of Service upon parsing Mime messages. Users are recommended to upgrade to version 0.8.15 which fixes the issue by enforcing new limits and providing better defaults.	7.5	More Details
CVE-2026-105002	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow arbitrary code to be executed by the management service in certain non-default configurations due to improper control of generation of code. Customization content may be evaluated as code, which is only possible where the related feature is enabled and not properly restricted.	7.5	More Details
CVE-2026-65983	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to 8.2.0, interface/modules/custom_modules/oe-module-faxsms/src/Controller/SignalWireClient.php decrypts a selected patient document with Document::get_data() and SignalWireClient::uploadFileForFax() writes the plaintext bytes under sites/{siteId}/fax. The module returns the resulting public URL to SignalWire, protects it only with a predictable uniqid() filename, and never removes the staged file. An unauthenticated network actor who obtains or guesses the URL can retrieve persistent patient documents even when drive encryption is enabled. This issue is fixed in version 8.2.0.	7.5	More Details
CVE-2026-105321	Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in Kobikom Telecommunications and Informatics Services Inc. Kobikom allows SQL Injection. This issue affects Kobikom: before KobiPBX-FOP3-SEC-r1.	7.5	More Details
CVE-2026-	Insertion of Sensitive Information Into Sent Data vulnerability in BAKKBONE Australia FloristPress bakkbone-florist-companion allows Retrieve Embedded Sensitive Data.This issue affects FloristPress: from n/a through 7.8.4.	7.5	More Details

119499			
CVE-2026-123095	mpv 0.29.0 before 0.42.0 contains a playlist injection vulnerability in the bundled ytdl_hook script that allows remote attackers to add unchecked entries by embedding newlines in playlist URLs. Attackers controlling a feed or page can bypass url_is_safe() to open file:// or av:// inputs, reading local files or loading shared objects via ladspa for code execution.	7.5	More Details
CVE-2026-123281	In JetBrains Datalore before 2026.4 notebook code could execute commands in the sidecar container via the mount broker	7.5	More Details
CVE-2026-120043	The Affiliate Program Suite — SliceWP Affiliates plugin for WordPress is vulnerable to generic SQL Injection via the 'email' parameter in all versions up to, and including, 1.2.14 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. The injection is reachable without any account because the vulnerable code path is triggered via the user_register hook fired on every successful WooCommerce My Account registration, which requires only a guest-obtainable nonce.	7.5	More Details
CVE-2026-111768	The Model Context Protocol TypeScript SDK provides TypeScript client and server implementations of the Model Context Protocol. From 1.3.0 until 1.32.0 in @modelcontextprotocol/sdk and from 2.0.0 until 2.3.0 in @modelcontextprotocol/server, HTTP servers did not enforce a limit on the number of array elements and object keys validated in one request. The affected surface is validation of HTTP requests containing arrays or object keys. The trigger is an array-element or object-key validation workload large enough to exhaust memory while remaining within the request size limit. A single request within the default 4 MiB limit can terminate the process with JavaScript heap exhaustion. No credentials are required unless the application authenticates before SDK processing. Tools accepting arrays or records carry the greatest risk. stdio-only servers do not expose the HTTP request path. Upgrading alone does not enable the new validation bound. Operators must configure both a tool-input element bound and an appropriate request body size limit. This issue is fixed in @modelcontextprotocol/sdk 1.32.0 and @modelcontextprotocol/server 2.3.0.	7.5	More Details
CVE-2026-19877	INFINITT ULite 5.0.2.1_BN48_20260528 and earlier protects image-share links with a low-entropy password and does not restrict repeated password attempts, allowing an unauthenticated remote attacker to brute-force the password within the link validity window and gain unauthorized access to shared medical images. Fixed in ULite 5.0.2.1 BN50.	7.5	More Details
CVE-2026-117525	The FV Flowplayer Video Player WordPress plugin before 7.5.57.7212 does not escape shortcode attribute values embedded in comments before rendering them into the media player markup, allowing an unauthenticated visitor to store a script payload in a comment that executes in the session of any visitor, including an administrator, who plays the commented video, when the non-default comment-shortcode-parsing setting is enabled.	7.5	More Details
CVE-2026-19128	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow an authenticated attacker to send unauthorized requests from the system due to server-side request forgery. This could be used to enumerate network resources or to support further attacks.	7.5	More Details
CVE-2026-121006	HTTP::Body versions before 1.24_02 for Perl parse the trailer in quadratic time. Everything after the last chunk in the same call to add() is parsed with HTTP::Headers, which takes time quadratic in the number of fields of one name. For example, it takes several seconds to parse 16 KiB of "a:" lines. A remote attackercan exhause the CPU with a single request. HTTP::Body version 1.25 limits the size and number of lines in the trailer.	7.5	More Details
CVE-2026-16714	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote attacker to overwrite arbitrary files due to a path traversal vulnerability.	7.5	More Details
CVE-2026-62126	Allocation of Resources Without Limits or Throttling vulnerability in miniOrange SAML SP Single Sign On miniorange-saml-20-single-sign-on allows HTTP DoS.This issue affects SAML SP Single Sign On: from n/a through 6.1.0.	7.5	More Details
CVE-2026-82894	Improper Authorization in ContentWorker in Apache OFBiz 24.09 before 24.09.08 on all platforms allows a remote unauthenticated attacker to trigger arbitrary OFBiz service invocation with attacker-controlled parameters, resulting in arbitrary file write, arbitrary file deletion, and server-side request forgery, by requesting the public showHelpPublic view against a Content row whose serviceName field an account holding only CONTENTMGR_CREATE or CONTENTMGR_UPDATE has set to an attacker-chosen service, causing ContentWorker.renderContentAsText to resolve the service to invoke from that persisted, client-writable field and build its parameters directly from the live HTTP request map with no allow-list, no ownership check, and no requirement that the caller be authenticated. Users are recommended to upgrade to version 24.09.08, which fixes this issue.	7.5	More Details
CVE-2026-56065	Insertion of Sensitive Information into Externally-Accessible File or Directory vulnerability in Doofinder Doofinder for WooCommerce doofinder-for-woocommerce allows Retrieve Embedded Sensitive Data.This issue affects Doofinder for WooCommerce: from n/a through 2.17.2.	7.5	More Details
CVE-	FastNetMon is a high-performance DDoS detector and sensor. In version 1.2.9 and earlier, the NetFlow v9 collector calls strlen() on an attacker-controlled interface-description field without bounding the scan to the		

2026-92697	field’s declared length. Although fields longer than 128 bytes are excluded from this operation, an accepted field without a null terminator can cause reads beyond the field and packet buffer. An unauthenticated remote attacker who can send crafted UDP packets to the collector can trigger an out-of-bounds read and potentially crash the process, causing denial of service. No fixed release is available as of this review.	7.5	More Details
CVE-2026-93424	FastNetMon is a high-performance DDoS detector and sensor. In version 1.2.9 and earlier, peer_find_template() in src/netflow_plugin/netflow_collector.cpp and src/netflow_plugin/netflow_v9_collector.cpp returns a pointer into global_netflow9_templates after releasing the cache mutex. On deployments with at least two entries in netflow_ports, concurrent template redefinition and data-flowset processing can let add_update_peer_template() reassign the template and free its records vector while another listener dereferences the escaped pointer. An unauthenticated sender that can reach both NetFlow/IPFIX listener ports can trigger a heap-use-after-free and reliably crash FastNetMon. No fixed release is available as of this review.	7.5	More Details
CVE-2025-71458	FTS3 Web Monitoring (fts-monitoring) versions 3.12.0 through 3.13.2 and 3.14.0 contain an unauthenticated sql injection vulnerability in the /linkinfo endpoint handled by get_linkinfo. Remote attackers can inject SQL through the source_se and dest_se query parameters to perform blind injection and read stored cloud storage credentials and token provider client secrets.	7.5	More Details
CVE-2026-77299	Regexp2 is a feature-rich RegExp engine for Go. Prior to version 2.3.0, when regexp2 compiles and matches a pattern containing a large fixed-count quantifier applied to a zero-width subexpression — e.g. (?:){50000000} — the match engine executes the empty loop body m-1 times, pushing two integers onto the backtracking stack on every iteration. Because the parser accepts any repetition count up to math.MaxInt32 and the backtracking stack grows without bound, a pattern of fewer than 20 bytes matched against an empty input can force multi-gigabyte allocation and OOM-kill the process. MatchTimeout does not fully mitigate this because the memory is allocated faster than the 100 ms timeout clock can fire. This issue has been patched in version 2.3.0.	7.5	More Details
CVE-2026-110813	The Advanced Custom Fields (ACF®) WordPress plugin before 6.8.11 does not properly sanitize a stored field definition that can be modified through its comment handling, allowing unauthenticated users to inject a payload that is emitted as an HTML attribute name and executed as JavaScript in the browser of any visitor or administrator who views a page rendering the affected field.	7.5	More Details
CVE-2026-62000	Missing Authorization vulnerability in WC Lovers WCFM Marketplace wc-multivendor-marketplace allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WCFM Marketplace: from n/a through 3.8.2.	7.5	More Details
CVE-2026-121817	Herowatch Go Server developed by About Time Technologies has a Insecure Direct Object Reference vulnerability. Authenticated remote attackers can modify specific parameters to access or operate other users' data and functions.	7.5	More Details
CVE-2026-115673	The Anti-Spam, Spam FireWall by CleanTalk WordPress plugin before 6.91 does not escape a commenter-supplied value before outputting it on an administrative spam-review screen, allowing unauthenticated users to inject arbitrary web scripts that execute in the browser of an administrator who reviews flagged comments.	7.5	More Details
CVE-2026-103112	A flaw was found in the authentication session handling of the keycloak-services component in Keycloak. The issue occurs because the system fails to verify if an authenticator is valid for the current authentication flow when switching between the standard authentication path and the reset credentials path. An authenticated attacker can exploit this by triggering a race condition during the credential reset process to associate their successful authentication state with another user's session. This can result in the attacker gaining full access to the victim's account and changing their password.	7.5	More Details
CVE-2026-107123	A flaw was found in the SAML XML processing component of Keycloak, an open-source identity and access management solution. The issue occurs when the server parses XML documents containing excessively long dateTime or duration values. Because these strings are not properly validated before processing, the XML parser consumes excessive CPU time. An unauthenticated remote attacker can exploit this by sending specially crafted SAML requests to the server, leading to high CPU utilization and a denial of service for all users.	7.5	More Details
CVE-2026-116782	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to 1.11.2, rtmp_i_connect() passed the first RTMP connect argument to amf0_object_get() without checking whether the AMF value was an object. A string or number in place of an AMF object caused union bytes from the message to be interpreted as node pointers and dereferenced. Any client with network access to an enabled mod_rtmp listener could send the malformed connect command before login; the module is disabled in the stock build and configuration. The invalid read reliably crashes FreeSWITCH and ends every active call, while no write, memory disclosure, or code execution has been demonstrated. This issue is fixed in version 1.11.2.	7.5	More Details
CVE-2026-86606	The iubenda | All-in-one Compliance for GDPR / CCPA Cookie Consent + more WordPress plugin before 3.13.7 does not properly escape content it re-emits through its bundled HTML parser, allowing unauthenticated users to inject arbitrary web scripts in pages that will execute in the session of any visitor viewing them, including logged in administrators.	7.5	More Details
CVE-2026-105325	Missing check for ACCOUNTING_UPDATE / ACCOUNTING_CREATE in accounting in allows user with only ACCOUNTING_VIEW permission to update/create PaymentApplication. Affected versions before : 24.09.08 Users are recommended to upgrade to version 24.09.08 which fixes this issue.	7.5	More Details

CVE-2026-105461	Missing check for ORDERMGR_UPDATE in ordermgr allows user with only ORDERMGR_VIEW permission to update orders. Affected versions before : 24.09.08 Users are recommended to upgrade to version 24.09.08 which fixes this issue.	7.5	More Details
CVE-2026-116784	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to 1.11.2, process_rtcp_report() used an RTPFB NACK packet's declared RTCP header length as its feedback-entry loop bound instead of the datagram length already validated by the caller. A short packet with an oversized declaration could drive reads far beyond the fixed 16 KiB receive buffer. Any peer able to send RTCP to an active video call can reach the flaw, including calls where remote SDP enables video RTCP even though the SIP profile has no explicit RTCP interval configured. The out-of-bounds read can crash FreeSWITCH and terminate every active call, but supplies no write primitive and does not echo the read values to the sender. This issue is fixed in version 1.11.2.	7.5	More Details
CVE-2026-123305	In JetBrains IntelliJ IDEA before 2026.3 path traversal was possible via unpacking Dev Container archives from a remote host	7.5	More Details
CVE-2026-82965	A flaw was found in the SAML implementation of Keycloak, an open-source identity and access management solution. The SAML Artifact Resolution and ECP SOAP endpoints do not properly limit the size or complexity of incoming XML requests. An unauthenticated remote attacker can exploit this by sending specially crafted, large XML messages that cause the server to consume excessive memory. This leads to the application running out of memory and crashing, resulting in a denial of service for all users.	7.5	More Details
CVE-2026-116787	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to 1.11.2, mod_event_socket used an unauthenticated Content-Length value directly as the allocation size for an Event Socket message body. Negative or extremely large values could overflow the terminator calculation or force an allocation failure through a helper that aborts the FreeSWITCH process. The header is parsed before the Event Socket password, so any host admitted by apply-inbound-acl can trigger termination with its first packet; the default loopback ACL limits ordinary installations to local clients. The outbound socket dialplan path is also affected when FreeSWITCH connects to a hostile application server, and process termination drops every active call until the service is restarted. This issue is fixed in version 1.11.2.	7.5	More Details
CVE-2026-123059	In Eclipse BaSyx Helm Charts version 2.2.0 of the `aas-basyx-v2-full` chart, deployments with the bundled Keycloak enabled store the client secret of the `basyx-technical-user` OAuth2 client in cleartext in a Kubernetes ConfigMap. This client uses the client-credentials grant and its service account holds the realm `admin` role. The chart correctly writes `keycloak.technicalUser.clientSecret` to a Kubernetes Secret, but the template `basyx-keycloak-realm.yaml` also substitutes the same value into the Keycloak realm-import JSON, which is stored in the ConfigMap `<keycloak.fullnameOverride>-realm`. A principal that can read ConfigMaps but not Secrets in the release namespace, such as a holder of the built-in Kubernetes `view` ClusterRole, can read the client secret from the ConfigMap. They can then exchange it at the Keycloak token endpoint for an access token with the `admin` role. That token grants full create, read, update, delete and execute rights on all BaSyx repositories and registries in the deployment. The bundled Keycloak is disabled by default. No fixed release of the `aas-basyx-v2-full` chart exists. Affected users should migrate to the `basyx` chart, or deploy without the bundled Keycloak and rotate the `basyx-technical-user` client secret.	7.5	More Details
CVE-2026-123151	A flaw was found in the GNU debugger (GDB). When GDB connects to a remote debug target, a malicious target can cause GDB to overflow a buffer on the stack while parsing the target's replies. This can crash GDB or potentially allow the target to execute arbitrary code in the GDB client process with the privileges of the user running GDB.	7.5	More Details
CVE-2026-82904	Uncontrolled Resource Consumption in ServiceMultiEventHandler in Apache OFBiz 24.09 before 24.09.08 on all platforms allows a remote unauthenticated attacker to pin a server request thread for an attacker-chosen number of synchronous service dispatches, up to the signed-integer maximum, by submitting a single small HTTP request whose parameter names encode a row count via the "o" suffix used by multi-form submissions, because UtilHttp.getMultiFormRowCount derives that count from the largest such suffix with no upper bound and ServiceMultiEventHandler.invoke then loops that many times calling dispatcher.runSync, with the request-map for getFinAccountTransRunningTotalAndBalances reaching this handler with no authentication or CSRF requirement on a stock deployment. Users are recommended to upgrade to version 24.09.08, which fixes this issue.	7.5	More Details
CVE-2026-111821	Improper input validation vulnerability in Apache ActiveMQ, Apache ActiveMQ KahaDB. A user can create a durable subscription with a clientId and subscription name that have a combined length > 65,535 (while separately being shorter) on a broker using KahaDB which can cause the broker to shutdown and be unrecoverable. This issue affects Apache ActiveMQ: from 6.0.0 before 6.3.3, before 5.19.12; Apache ActiveMQ KahaDB: from 6.0.0 before 6.3.3, before 5.19.12. Users are recommended to upgrade to version 6.4.0, 6.3.3 or 5.19.12, which fixes the issue.	7.5	More Details
CVE-2026-73578	Missing authorization enforcement in RequestHandler.renderView in Apache OFBiz 24.09 before 24.09.08 on all platforms allows a remote unauthenticated attacker to bypass the request-map authentication policy for protected views by supplying a crafted _LAST_VIEW_NAME_ value, which is stored as saved-view state in the anonymous session and later rendered without re-applying the original view's authentication requirement, potentially exposing protected views and associated business data. Users are recommended to upgrade to version 24.09.08, which fixes this issue.	7.5	More Details

CVE-2026-121995	A stack buffer overflow in the GDB client's tracepoint upload handler allows an attacker-controlled debug stub to corrupt stack memory automatically during connection setup. The overflow results from GDB reading beyond the current reply boundary into a stale prior reply in the shared packet buffer.	7.5	More Details
CVE-2026-123296	In JetBrains Hub before 2026.2.52519 privilege escalation via forged email verification was possible	7.5	More Details
CVE-2026-77604	Code Graph RAG is an AI-powered knowledge graph and retrieval system for querying, understanding, and editing multi-language codebases. Prior to 0.0.345, the MCPToolsRegistry.read_file implementation in codebase_rag/mcp/tools.py joins attacker-controlled file_path input to project_root without resolving and verifying containment when offset or limit selects the paginated branch. An absolute path causes pathlib to discard the configured root, while relative traversal can also resolve outside it. The protected non-paginated branch uses validate_project_path, but the paginated branch bypasses that validation before opening the path. An unauthenticated caller of a network-exposed HTTP MCP server can therefore read arbitrary UTF-8-readable files available to the server process, including credentials, environment data, private keys, source, and configuration; local callers through the stdio transport can reach the same vulnerable code path. This issue is fixed in version 0.0.345.	7.5	More Details
CVE-2026-106713	An issue in FreeReels for Android version 2.3.11 allows a remote attacker to obtain sensitive information via the com.dramawave.feature.web.WebPageActivity component	7.5	More Details
CVE-2026-110932	A flaw was found in the theme resource endpoint of Keycloak, an open-source identity and access management solution. The issue occurs because the server fails to validate theme names before using them as keys for an on-disk gzip cache. An unauthenticated attacker can exploit this by sending many requests with unique, fabricated theme names, leading to persistent disk space exhaustion that survives server restarts and causes service disruptions.	7.5	More Details
CVE-2026-110931	A flaw was found in the SAML 1.1 assertion parser of Keycloak, a tool used for identity and access management. The issue occurs when the parser handles a specific element called AuthorityBinding within an authentication statement. Due to an incomplete fix for a previous vulnerability, the parser can enter an infinite loop that consumes all available memory, causing the entire Keycloak service to crash and become unavailable to users.	7.5	More Details
CVE-2026-68524	An unauthenticated attacker can exploit temporary-file handling, access an open file descriptor, and inject a "file:" URI to cause OFBiz to load an attacker-controlled Screen definition. This issue affects Apache OFBiz: before 24.09.08. Users are recommended to upgrade to version 24.09.08, which fixes the issue.	7.5	More Details
CVE-2026-107602	A flaw was found in the SAML 1.1 XML parsing logic of Keycloak, an open-source identity and access management solution. The issue occurs when the parser encounters unexpected elements within a security token's key information section, causing the processing thread to enter an infinite loop. An unauthenticated remote attacker could exploit this by sending specially crafted requests, leading to 100% CPU usage and a total denial of service that requires a server restart to resolve.	7.5	More Details
CVE-2026-73577	Incorrect authorization in RequestHandler in Apache OFBiz 24.09 before 24.09.08 on all platforms allows a remote unauthenticated attacker to bypass the authentication requirement of a protected view by appending it as a path suffix to a public request (e.g., /catalog/control/ListLocales/showPortalPage), causing the servlet to authorize the request based on the public path component while rendering the protected suffix view. Users are recommended to upgrade to version 24.09.08, which fixes this issue.	7.5	More Details
CVE-2026-17331	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote attacker to read arbitrary files on the server due to external control of a file name or path.	7.5	More Details
CVE-2026-104768	The AutomatorWP – No-Code Workflow Automation, Integration & Webhooks Plugin, now with AI plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 6.0.4. This is due to missing privilege-ceiling validation in the `create_user()` function within the anonymous-user action (and equally in the Create User and Add/Change Role WordPress-integration actions), which verify only that the submitted role exists via `automatorwp_get_editable_roles()` without confirming the role falls at or below the acting context's privilege level — allowing attacker-controlled trigger tag data (e.g., a `{comment_author}` tag bound to the Role option) to supply any role, including `administrator`, unchallenged. This makes it possible for unauthenticated attackers to create a new administrator-role account tied to an attacker-controlled email address, receiving the generated password via WordPress's new-user notification email and thereby gaining full administrative access to the site. Exploitation requires the site to have an anonymous automation configured with the Role option bound to a dynamic trigger tag such as `{comment_author}`, and is triggered when a site administrator performs the routine action of approving a comment — an action that provides no in-UI indication that it will mint a new privileged account from the comment author field.	7.5	More Details
CVE-2026-10859	IBM MQ 9.2.0.0 through 9.2.0.44 LTS, 9.3.0.0 through 9.3.0.42 LTS, 9.4.0.0 through 9.4.0.26 LTS, 9.4.0.0 through 9.4.5.1 CD, and 10.0.0.0 through 10.0.0.5 LTS and CD could allow an authenticated attacker to execute arbitrary code on consumer applications due to insecure deserialization of ObjectMessage payloads.	7.5	More Details
	Nuxt Content is the file-based CMS for Nuxt applications, powered by Markdown and Vue components. From 3.0.0 until 3.15.2, the unauthenticated POST /__nuxt_content/:collection/query endpoint accepts an attacker-controlled		

CVE-2026-102650	sql field in src/runtime/api/query.post.ts and permits expensive SQLite expressions. Version 3.0.0 performed no query validation; in affected releases using assertSafeQuery in src/runtime/internal/security.ts, the reported validation gap rejects a short list of SQL command keywords in WHERE clauses but permits function calls including randomblob(), zeroblob(), hex(), and length(). The query reaches the synchronous better-sqlite3 sink in src/runtime/internal/database.server.ts, allowing a single remote request to consume substantial CPU and memory while blocking the Node.js event loop and all concurrent request handling. Fully static prerendered deployments that do not expose the server endpoint are not affected. This issue is fixed in version 3.15.2.	7.5	More Details
CVE-2026-85742	FreeScout is a self-hosted help desk and shared mailbox. Prior to 1.8.230, a pre-authenticated attacker can place HTML in a failed-login email value that is copied through monitored user activity into a queued SendAlert job. If alert delivery fails, the serialized payload is stored in failed_jobs and the administrator job-details endpoint renders it after a blacklist sanitizer that leaves executable event-handler attributes. When an administrator opens /system/ajax-html/job_details/{id} as a top-level page, the raw fragment lacks the normal layout policy and attacker-controlled JavaScript can perform same-origin administrator actions. Logs Monitoring for users, a failed alert email job, queue failure storage, and top-level administrator interaction are all required; the normal modal path is not affected in the tested configuration. This issue is fixed in version 1.8.230.	7.5	More Details
CVE-2026-89017	Skyline DataMiner BrokerGateway contains an embedded API key vulnerability that allows unauthenticated attackers to retrieve the installation-specific BrokerGateway key even while pairing mode is disabled. Attackers can use the retrieved key to obtain the unrestricted DataMinerUser.creds NATS credential and gain trusted message-bus access via TCP port 4222 without any prior DataMiner credentials. Fixed in DataMiner 10.6.9 CU1, 10.6.0 CU7, 10.5.0 CU19, and 10.4.0 CU22.	7.5	More Details
CVE-2026-124027	ChatWiki before 2.10.0 contains a missing authentication vulnerability in the GET /manage/getLibRawFileOnePage route that allows unauthenticated attackers to read other tenants' documents. Attackers can enumerate sequential admin_user_id and file id query parameters, bypassing the ownership check, to retrieve PDF-rendered pages of any tenant's knowledge-base documents.	7.5	More Details
CVE-2026-120645	CGI versions before 5.00 for Perl allow denial of service via submitted values used as a regex for optgroup selection in scrolling_list. When rendering option groups, scrolling_list marks the selected options by interpolating each selected value, by default taken from the request parameters, unescaped into a substitution pattern. A client can make the request die with an invalid pattern, or tie up the process with one that backtracks heavily.	7.5	More Details
CVE-2026-17493	IBM Watson Speech Services Cartridge 4.0.0 through 5.4.0 could allow a remote attacker to cause a denial of service due to an out-of-bounds read.	7.5	More Details
CVE-2026-119749	The GetPaid plugin for WordPress before 2.8.63 contains an improper input validation vulnerability that allows unauthenticated attackers to bypass payment processing by submitting a negative item quantity on a public payment form. Attackers can exploit the unchecked quantity value in process_item() to produce a negative line subtotal that reduces the invoice total to zero, causing process_free_payment() to mark the invoice as paid without any actual gateway charge.	7.5	More Details
CVE-2026-109991	The FunnelKit Payment Gateway for Stripe WooCommerce plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 1.15.0.2 via the 'order-pay (WP query var from /checkout/order-pay/<ID>/)' parameter due to missing validation on a user controlled key. This makes it possible for unauthenticated attackers to read the full billing PII — including name, email address, phone number, and complete street address — of any store order by enumerating sequential order IDs, as this data is emitted into the inline fkwcs_data JavaScript object via wp_localize_script on every matching page response. Exploitation occurs even when WooCommerce itself rejects the order-pay page request, because the plugin's wp_localize_script call runs independently of WooCommerce's own order-key validation on the same request.	7.5	More Details
CVE-2026-102657	esm.sh is a no-build content delivery network (CDN) for web development. Prior to server version 137_7, the documented web.NewHandler static file server in web/handler.go joins the URL-decoded r.URL.Path with Config.AppDir without verifying that the result remains inside the configured application directory. URL-encoded dot segments such as %2e%2e bypass the plain traversal redirect performed by Go's ServeMux, allowing an unauthenticated remote attacker to make the server open and return files outside Config.AppDir that are readable by the server process. The confirmed impact is file disclosure only, and the issue is reachable with Dev disabled. This issue is fixed in server version 137_7.	7.5	More Details
CVE-2026-123855	In JetBrains Toolbox App before 3.6.1 command injection was possible via enterprise configuration URLs	7.5	More Details
CVE-2026-121964	FreeRDP before 3.32.2 contains a heap-based buffer overflow in the RD Gateway RPC client, where rpc_client_recv_fragment writes BIND_ACK and ALTER_CONTEXT_RESP fragments into a persistent PDU stream after checking only total capacity rather than remaining capacity from the current stream position. A malicious or compromised RD Gateway can send crafted RPC fragments with manipulated alloc_hint and frag_length values to overwrite client heap memory with attacker-controlled data, causing a crash or potentially arbitrary code execution.	7.5	More Details
CVE-2026-121960	FreeRDP before 3.32.2 contains a denial of service vulnerability in the NLA-enabled shadow server when a CredSSP TSRequest omits negoTokens. Unauthenticated attackers can send a crafted seven-byte TSRequest containing only the version field to trigger a fatal WINPR_ASSERT and abort the server process.	7.5	More Details

CVE-2026-82308	A pre-authentication heap-based buffer overflow vulnerability has been identified in the SonicOS SSL-VPN service, which could potentially enable a remote unauthenticated attacker to cause an application level denial of service.	7.5	More Details
CVE-2026-121957	FreeRDP before 3.32.2 contains a use-after-free vulnerability that allows malicious RDP servers to corrupt client memory by racing the RDPGFX ResetGraphics handler against the planar bitmap decoder. Attackers can send ResetGraphics while concurrently sending compressed bitmaps of 32 bpp or more to trigger heap use-after-free or out-of-bounds read/write on shared planar buffers.	7.5	More Details
CVE-2026-121956	FreeRDP before 3.32.2 contains a double free in the WinPR Kerberos SSPI retrieveSomeTgt function, which installs the krb5 default realm into a target principal that has an empty realm without taking ownership of it. Unauthenticated remote clients can send a crafted NLA/CredSSP u2u TGT request whose server-name component contains '@' to corrupt the heap and crash the server process.	7.5	More Details
CVE-2026-121955	FreeRDP before 3.32.2 contains a use-after-free vulnerability in Emulate_SCardReleaseContext that frees the emulated SCardContext before its worker thread is cancelled and joined. A malicious server can send ESTABLISHCONTEXT, a long-timeout GETSTATUSCHANGE, then RELEASECONTEXT smartcard IRPs to corrupt heap memory or crash clients using smartcard emulation.	7.5	More Details
CVE-2026-54381	VitaFit cloud API before 2026-10-30 contained a misconfigured cloud storage bucket vulnerability that allows unauthenticated attackers to list and download stored files without authentication. Attackers can enumerate the publicly accessible bucket containing 129,947 objects, including 126,881 user-uploaded profile images, to access sensitive personal data without credentials.	7.5	More Details
CVE-2026-123620	Usermin through 2.570 contains an OS command injection vulnerability in the Read Mail module that allows authenticated users to execute commands through unsanitized IMAP folder names. Attackers can create a folder containing shell metacharacters via an external IMAP client, then delete it in Usermin to run commands as their system account, bypassing webmail-only restrictions.	7.5	More Details
CVE-2026-85708	Chartbrew is an open-source web application that can connect directly to databases and APIs and use the data to create charts. Prior to 5.2.3, Chart share and embed tokens were signed with CB_SECRET, including known or shipped-default values in stock source and repository Docker Compose installs. The vulnerable surface is chart share-token verification and filter-access routes for private charts. An attacker who knows the deployment's CB_SECRET targets a private chart that has been shared at least once so a share-policy row exists, then forges a Chart-subject token for that chart id. The known signing key permits valid Chart tokens, and the filter-access path accepts sequential integer ids without requiring a legitimate share link; token expiry and revocation are ineffective once the secret is known. The condition requires a known or default secret and an existing share-policy row. A bare container where CB_SECRET is undefined is outside this path, and a unique secret excludes it only while the value remains unknown and unpredictable. An unauthenticated attacker can enumerate integer ids and read arbitrary private chart data, including chartData, without possessing a legitimate share link. This issue is fixed in version 5.2.3.	7.5	More Details
CVE-2026-103582	Unbounded memory allocation and missing frame size validation in Apache NMS ActiveMQ (the .NET OpenWire client, package Apache.NMS.ActiveMQ) before 2.3.0. The OpenWire unmarshalling code trusted the frame size and the length and count fields read from the network. It did not enforce a maximum frame size, and it did not check that decoded lengths fit within the frame being read. A malicious or compromised broker, or an attacker able to intercept and modify an unencrypted connection, could send a crafted OpenWire frame with an oversized or negative length. This could cause the client to attempt very large memory allocations, leading to excessive memory consumption, an OutOfMemoryException or an uncaught exception, and a denial of service of the client application. Users are recommended to upgrade to version 2.3.0, which enforces a configurable maximum frame size and validates lengths against the size of the frame being read.	7.5	More Details
CVE-2026-121951	FreeRDP 3.0.0 before 3.32.2 server-side RDP peer input parsing skips the six-byte body of a slow-path input event with an unknown message type without checking it lies within the packet's declared length, causing a WinPR stream assertion failure. A remote RDP client with an active session can send a truncated unknown input event to abort assertion-enabled server processes, causing denial of service.	7.5	More Details
CVE-2026-87045	The HTTP/2 server in subsys/net/lib/http/http_server_http2.c clears the connection's stream binding at the start of every frame. handle_http_frame_header() executed client->current_stream = NULL unconditionally, but a CONTINUATION frame does not open a new stream and enter_http_frame_continuation_state() never re-bound one, so the rest of the header block was processed with client->current_stream unset. Two paths then write through the NULL pointer. A request for an unregistered resource, or a method the matched resource does not support, is answered by send_http2_404() or send_http2_405(), and both call send_headers_frame(), which unconditionally sets client->current_stream->headers_sent = true. A POST, PUT or PATCH to a registered dynamic resource reaches handle_http2_dynamic_resource(), which unlike its siblings (handle_http2_static_resource(), dynamic_get_del_opts_req_v2(), dynamic_post_put_req_v2()) had no client->current_stream == NULL guard, and stores through the pointer with client->current_stream->current_detail = dynamic_detail. Any peer that can reach the server can trigger this without authentication or prior state. A single stray CONTINUATION frame with END_HEADERS set, sent right after the client preface and requesting any unregistered path, is enough, because nothing rejected a CONTINUATION that no HEADERS frame had opened. A legitimate split header block (a HEADERS frame with END_HEADERS clear whose payload ends on a header-field boundary, then a CONTINUATION with END_HEADERS set) reaches the same state. The in-tree test test_http2_post_headers_with_continuation() did not catch this because it splits the header block mid field, which takes the handle_incomplete_http_header() shortcut that keeps the stream bound. The result is a write to a fixed	7.5	More Details

	low address (a small offset into struct http2_stream_ctx), which faults on mainstream targets (flash/vector-table region on Cortex-M, or a trap under MPU/MMU null-pointer detection), and the default fatal-error handler halts the system. Impact is an unauthenticated, remotely triggerable denial of service against any device running the HTTP/2 server: the 404 path needs no particular resource to be registered, and HTTP/2 is built into CONFIG_HTTP_SERVER with cleartext h2c accepted, so TLS does not prevent it. Neither the target address nor the written value is attacker-controlled, so there is no confidentiality or integrity impact. Applications built without CONFIG_HTTP_SERVER are not affected.		
CVE-2026-54374	VitaFit Android application (com.vt.vitafit) before 2.8.1.0 contains a hardcoded credentials vulnerability that allows attackers to extract confidential third-party integration secrets by decompiling the APK. Attackers can retrieve embedded WeChat, Tencent QQ, and Fitbit credentials from the decompiled application to abuse the active third-party application registrations.	7.5	More Details
CVE-2026-106554	One CBOR-parsing issue in jackson-dataformats-binary's CBOR module: an unbounded run of CBOR tags drives quadratic-time TagList growth (CPU/GC-exhaustion DoS, PoC-proven). PoC executed against com.fasterxml.jackson.dataformat:jackson-dataformat-cbor:2.18.2; present in current 2.x and 3.x (tools.jackson.dataformat.cbor) HEAD. Distinct from the Avro and Smile/Protobuf advisories for this repo. Quadratic CPU/GC DoS from an unbounded chain of CBOR tags (PoC-proven). File: cbor/src/main/java/.../cbor/CBORParser.java (tag handling -> TagList). CBOR permits a data item to be preceded by any number of semantic tags. The CBOR parser accumulates them in a TagList whose backing array grows by a fixed increment (+8), not by doubling, and re-scans/copies on each growth. An attacker sends a value preceded by a long run of tag bytes; the fixed-increment growth makes accumulating N tags O(N^2) in time (plus GC pressure), with no cap on the number of stacked tags. PoC (executed, JDK 17): feeding a CBOR stream consisting of a long run of tag bytes (e.g. tag 0xC0+) before a trivial value forces quadratic CPU/GC; parse time grows super-linearly with the tag count, pinning a request thread with no configurable limit. Impact. Algorithmic-complexity denial of service (CWE-407): a modest input of stacked tags consumes quadratic CPU/GC, pinning a request thread; concurrent requests exhaust the pool. Fix. Grow TagList by doubling and/or cap the number of stacked tags (StreamReadConstraints-style).	7.5	More Details
CVE-2026-123356	GROBID is machine learning software for extracting information from scholarly documents. Prior to 0.9.1, the unauthenticated /api/modelTraining endpoint calls GrobidRestProcessTraining.trainModel in GrobidRestProcessTraining.java, where each request creates Executors.newFixedThreadPool(1), submits a training task, and leaves the executor running. Repeated requests permanently retain JVM worker threads and can exhaust process or operating-system thread capacity, degrading or stopping request processing. This issue is fixed in version 0.9.1.	7.5	More Details
CVE-2026-55367	h2o is an HTTP server with support for HTTP/1.x, HTTP/2 and HTTP/3. Prior to commit 4212ce114506a073505fd389db16ad2ba4e582a0, a client could send an incomplete CONNECT-UDP Capsule with an excessively large declared length, causing H2O to keep buffering received bytes without a per-Capsule limit while waiting for the remainder. Deployments that enabled proxy.connect-udp and accepted CONNECT-UDP requests could exhaust server memory and lose availability. This vulnerability is fixed with commit 4212ce114506a073505fd389db16ad2ba4e582a0.	7.5	More Details
CVE-2026-19868	An authentication enforcement vulnerability in SonicOS SSLVPN service may allow a user with valid credentials for an alternate authentication method to bypass SAML authentication controls. Successful exploitation may also bypass SAML-enforced multi-factor authentication (MFA).	7.5	More Details
CVE-2026-63655	tsParticles is a TypeScript library for creating highly customizable particle animations. Prior to 4.3.1, the HTTP mode of @tsparticles/mcp-server accepts unauthenticated POST /mcp requests in integrations/mcp-server/src/index.ts and accumulates every request-body chunk in a Buffer[] without a cumulative size limit before Buffer.concat and JSON.parse. A remote attacker can stream an arbitrarily large body to exhaust Node.js process memory and terminate the service, including in the official Docker configuration that exposes HTTP mode on 0.0.0.0:3000. Confidentiality and integrity are not affected. This issue is fixed in version 4.3.1.	7.5	More Details
CVE-2026-62344	Wanderer is a self-hosted trail database for saving and sharing adventures. Prior to 0.19.3, the unauthenticated GET /activitypub/trail/{id} and GET /activitypub/comment/{id} endpoints call ActivitypubTrail() and ActivitypubComment() to return full trail and comment records without applying the PocketBase collection view rules. An attacker who can enumerate or guess record IDs can retrieve private trail names, descriptions, GPS coordinates, GPX file URLs, photo URLs, and comments. This issue is fixed in version 0.19.3.	7.5	More Details
CVE-2026-124078	plist.js (npm package 'plist') before 5.0.1 contains an uncontrolled resource consumption vulnerability in the binary property-list parser (parseBinary) that allows unauthenticated attackers to crash a Node.js process by exploiting unmemoized recursive resolution of shared object references for arrays and dictionaries. Attackers can craft a small binary plist (under 200 bytes) containing chained self-referencing object indices to trigger exponential (2^N) resolution calls and memory growth, causing an unrecoverable out-of-memory crash and denial of service.	7.5	More Details
CVE-2026-122192	Improper handling of a failed memory remap in Firecracker versions 0.23.0 through 1.16.1 might allow a guest user with root privileges to read or modify Firecracker VMM process memory via balloon or virtio-mem discard requests on microVMs restored from a snapshot with the File memory backend, if the host fails to create the replacement mapping. To remediate this issue, users should upgrade to Firecracker 1.16.2 or 1.17.0 and later.	7.5	More Details
	Chartbrew is an open-source web application that can connect directly to databases and APIs and use the data to		

CVE-2026-85726	create charts. Prior to 5.2.3, a date-typed MongoDB variable placed inside a quoted query placeholder was inserted as an unescaped string, unlike the safely escaped or coerced string, number, and Boolean branches. The vulnerable surface is mongoDB-backed public, shareable, or embedded charts processed by date-variable substitution. An unauthenticated user supplies a crafted URL filter to a public, shareable, or embedded MongoDB chart whose query places a date-typed variable in a quoted literal. The crafted date value breaks out of the quoted literal and changes query logic; the chart's returned row count becomes a Boolean oracle for character-by-character field extraction. The chart must be externally reachable and use the vulnerable date-in-quoted-placeholder branch. Extraction is read-only and limited to one queried collection per request, and it requires neither an account nor a known field value. The blind oracle can disclose any field in the queried collection, including secrets the chart does not display. This issue is fixed in version 5.2.3.	7.5	More Details
CVE-2025-66366	Incorrect handling of unauthenticated downlink RRC Setup messages can cause the baseband to crash	7.5	More Details
CVE-2026-104203	Traccar is an open source GPS tracking system. From 5.1 until 6.15.0, WebModule.java's MediaFilter Guice mapping and WebServer.java's Jetty ResourceServlet assign different routing meanings to path parameters at /api/media/*. An unauthenticated attacker who knows or guesses a device unique ID and media filename can insert a semicolon at the Servlet boundary, bypass MediaFilter's session and device authorization checks, and retrieve the protected media because Jetty still dispatches the noncanonical path to ResourceServlet. The demonstrated impact is read-only disclosure of a protected device media file; depending on the deployment and stored media, this could expose photographs, audio, video, or other uploaded files. The advisory does not establish directory listing, traversal, modification, account takeover, denial of service, or code execution. Reverse proxies that reject or rewrite semicolon path parameters may block the request. This issue is fixed in version 6.15.0.	7.5	More Details
CVE-2025-66368	Incorrect handling of SDP payload leads to a Denial of Service	7.5	More Details
CVE-2026-122127	CESNET ipfixcol2 2.7.1 before 2.9.0 contains a heap-based buffer overflow in Lz4Decoder.cpp that allows unauthenticated network peers to write past heap buffers. Attackers can declare a small ring buffer_size followed by a large decompressed_size to write up to 65535 controlled bytes and crash the collector.	7.5	More Details
CVE-2026-123487	Parse Server before 8.6.115 and 9.0.0 before 9.10.7-alpha.1 validates user email address format with a regular expression whose run time grows quadratically with input length and that is applied without a length limit. An unauthenticated attacker who knows the application ID can send a sign-up request, or a logged-in user can update their own email, with a long crafted email address to block the Node.js event loop and deny service to all clients.	7.5	More Details
CVE-2026-123834	In JetBrains Datalore before 2026.4 improper scope validation in database tasks allowed using another workspace's service account	7.5	More Details
CVE-2025-66364	Continuously sending control-plane messages causes the baseband to crashes.	7.5	More Details
CVE-2026-120646	CGI versions from 4.71 before 5.00 for Perl allow denial of service via a plain string dereferenced as a symbolic reference in uploadInfo. uploadInfo dereferences its argument and calls its filename method without checking that it is an upload filehandle. A plain string naming a defined global variable, such as the parameter value from ?upload=0, is treated as a symbolic reference, and the method call on it dies.	7.5	More Details
CVE-2026-97705	Moleculer is a progressive microservices framework for Node.js. Prior to 0.14.36 and 0.15.2, Parser._write in src/transporters/tcp/parser.js used Buffer.prototype.readInt32BE to read a signed packet length, so a remote unauthenticated peer could supply a negative value that caused packet.slice(length) to return the unchanged buffer while the while (packet.length > 0) loop continued indefinitely. The synchronous loop blocked the Node.js event loop and made every service in the process unresponsive until restart. The TCP transporter must be enabled and reachable, and neither CRC validation nor maxPacketSize prevents the malformed length value. This issue is fixed in versions 0.14.36 and 0.15.2.	7.5	More Details
CVE-2026-104657	Missing integrity verification in the Progress Software Fiddler Download and Setup Skill on Linux, macOS, and Windows which allows an attacker to compromise or influence a release component and execute attacker-controlled code when a user runs the skill. On macOS, the skill stages the package at a predictable path and installs it with administrator privileges, which may allow code execution with root privileges after user approval. A local process may also replace the staged macOS package while the skill waits for approval.	7.5	More Details
CVE-2026-95870	The wpForo Forum plugin for WordPress is vulnerable to generic SQL Injection via the 'data' parameter in all versions up to, and including, 3.2.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. Exploitation requires that a searchable topic form field of type checkbox, or a select/autocomplete field with isMultiChoice enabled, is registered in the forum configuration.	7.5	More Details

CVE-2025-66367	Improper handling of NAS DLTransport messages may lead to a baseband crash.	7.5	More Details
CVE-2026-102359	Kroki creates diagrams from textual descriptions. Prior to 0.31.2, the TikZ backend's tikz/tikz2svg guard used when KROKI_SAFE_MODE is enabled blocks only \verbatiminput while allowing native TeX file-read primitives including \openin, \read, \input, and \include. TeX Live's permissive openin_any setting remains active, so an unauthenticated actor can submit crafted LaTeX to POST /tikz/svg or the generic diagram API and cause the renderer to read any file accessible to the Kroki container user. The file contents are rendered into the returned SVG, which may disclose mounted secrets, configuration data, credentials, private keys, or process environment data. The -no-shell-escape option prevents shell execution but does not restrict these native file operations. This issue is fixed in version 0.31.2.	7.5	More Details
CVE-2026-12356	IBM MQ 9.2.0.0 through 9.2.0.44 LTS, 9.3.0.0 through 9.3.0.42 LTS, 9.4.0.0 through 9.4.0.26 LTS, 9.4.0.0 through 9.4.5.1 CD, and 10.0.0.0 through 10.0.0.5 LTS and CD could allow an authenticated user with command queue access to execute arbitrary code by injecting malicious arguments into Ant script commands.	7.5	More Details
CVE-2026-120631	CGI::Cookie versions from 4.67 before 5.00 for Perl allow denial of service via the client cookie expires value used as a regex in parse. CGI's cookie method reads the Cookie request header through parse, which interpolates the header's expires value unescaped into the substitution pattern that removes it from the cookie string. A client can make the request die with an invalid pattern, or tie up the process with one that backtracks catastrophically.	7.5	More Details
CVE-2026-17337	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to bypass authentication due to improper certificate validation. A certificate check is not performed reliably in all cases, which could allow a connection to be accepted without proper authentication.	7.4	More Details
CVE-2026-123282	In JetBrains Datalore before 2026.4 missing expiration validation of account tokens allowed a new authenticated session	7.4	More Details
CVE-2026-116592	undici is an HTTP client for Node.js. In versions 7.30.1 and 8.12.2 through 8.12.3, when an originless Agent composes the redirect and shared cache interceptors, undici decides whether to store the final response under the original request key by inspecting only the final redirect hop, which bypasses the earlier fix for CVE-2026-109829 that compared only the initial and final origins. A redirect that bounces through an untrusted origin and returns to the trusted origin is still cached under the trusted key, an intermediate hop's Vary is dropped so a response that varies on Authorization or Cookie can be served to a different user, and an intermediate hop's no-cache or default-uncacheable status is ignored so a non-storable redirect is laundered into a cacheable entry. An attacker who controls a redirect target from a trusted URL can poison the cached entry for that URL or have a private, per-user response served to a later caller. The issue is fixed in undici 7.30.2 and 8.12.4, and users should upgrade to one of those versions or later. As a workaround, compose the interceptors as cache then redirect, use per-origin dispatchers and cache stores, or disable shared caching on redirect-capable requests.	7.4	More Details
CVE-2026-109928	Incorrect Implementation of Authentication Algorithm in the password-reset and login JWT validation in Apache OFBiz 24.09 before 24.09.08 on all platforms allows an attacker who has obtained a user's password-reset token (via email interception, log exposure, or a man-in-the-middle on the mail transport) to authenticate as that user and obtain a full, unrestricted session, including administrative access if the targeted account is an administrator, by submitting the token directly to the login endpoint instead of the intended password-change flow. Users are recommended to upgrade to version 24.09.08, which fixes this issue.	7.4	More Details
CVE-2026-113783	ESP-IDF is the Espressif Internet of Things (IOT) Development Framework. From 5.2.3 until 5.3.7, 5.4.5, 5.5.6, and 6.0.3, the lwIP DNS resolver's cached-lookup path in dns_lookup() in dns.c copies every cached address into a caller-provided single ip_addr_t output buffer without a length parameter or bounds check. When CONFIG_LWIP_DNS_MAX_HOST_IP is greater than 1 and a cached hostname has multiple A or AAAA records, a subsequent lookup through dns_gethostbyname() or dns_gethostbyname_addrtype() writes beyond the single-element buffer into adjacent stack memory. A network-positioned attacker who influences DNS responses can cause a reboot through stack-canary corruption or, without stack protection, overwrite stack variables with attacker-controlled address bytes and potentially redirect control flow. This issue is fixed in versions 5.5.6 and 6.0.3 and is scheduled to be fixed in versions 5.3.7 and 5.4.5. No fixed release is available for the end-of-life 5.2 line.	7.4	More Details
CVE-2026-17379	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote attacker to bypass authentication and assign arbitrary roles due to improper verification of cryptographic signatures.	7.4	More Details
CVE-2026-123848	In JetBrains IntelliJ IDEA before 2026.3 host name verification was missing for server TLS certificates	7.4	More Details
CVE-2026-92855	A flaw was found in the SAML identity broker component of Keycloak, which is used to delegate authentication to external identity providers. The issue occurs because the broker fails to verify that a user actually possesses the private key associated with a holder-of-key assertion. An attacker who intercepts a victim signed assertion can replay it to gain unauthorized access and impersonate the victim without needing their private key.	7.4	More Details
CVE-	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to perform unauthorized actions and obtain sensitive information due to missing authorization. Certain		More

2026-17244	operations do not verify that the user is permitted to act on the targeted resource, which could allow other users' API keys to be deleted.	7.4	Details
CVE-2026-123852	In JetBrains Junie GitHub Action before 1.8.0 code execution with workflow credentials was possible via fork updates	7.4	More Details
CVE-2026-122118	In certain Yealink products before 2026-04-15, when the Wi-Fi AP function is enabled, a default 8-digit numeric PSK with insufficient strength is used. Attackers can exploit this weakness via brute-force attacks to gain unauthorized network access and intercept Wi-Fi traffic.	7.4	More Details
CVE-2026-93998	A flaw was found in the SAML adapter component of Keycloak, which is used to secure applications with SAML-based authentication. The adapter fails to verify that the issuer of a signed SAML assertion matches the expected identity provider configured for the application. If multiple identity providers share the same trusted signing key, an attacker who controls one of those providers can create a validly signed assertion to log into the application as any user, potentially gaining full administrative control.	7.4	More Details
CVE-2026-122220	WPO365 | LOGIN (wpo365-login) plugin before version 45.2 contains an authentication bypass by capture-replay vulnerability caused by a non-functional anti-replay check in Saml2_Service::check_message_id(), which never persists processed SAML message IDs to the wpo365_saml_message_ids transient due to a logic error that returns before saving. Attackers who capture a validly-signed SAMLResponse can replay it to the ACS endpoint repeatedly within its assertion validity window to log in as the victim, including administrators, without detection since the duplicate message ID check never triggers.	7.4	More Details
CVE-2026-116789	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to 1.11.2, dtls_state_setup() compared a peer certificate with the SDP a=fingerprint only when FreeSWITCH was the DTLS client, not when it held the DTLS server role. An unauthenticated peer able to reach the negotiated media port could complete the DTLS-SRTP handshake with an unrelated certificate, obtain the leg's SRTP keys, decrypt and inject media, and displace the legitimate endpoint; on ICE-enabled legs the peer also needs the connectivity-check credentials from SDP, which generally requires signaling visibility or a position on its path. WebRTC and SIP DTLS-SRTP legs are affected whenever the peer selects the active role, while FreeSWITCH client-role handshakes already perform fingerprint validation. Version 1.11.2 introduces the remediation, which requires rtp_dtls_client_cert_verify_mode=fingerprint.	7.4	More Details
CVE-2026-123306	In JetBrains IntelliJ IDEA before 2026.3 improper checks allowed server certificates to be added to the trust store during headless runs	7.4	More Details
CVE-2026-109408	vault-java-driver, a Java client for HashiCorp Vault, silently disables TLS certificate and hostname verification in three states where the caller asked for verification: an SslConfig passed to VaultConfig without calling build(), an SslConfig restored by Java deserialization, and VAULT_SSL_VERIFY set to a truthy value other than "true", such as 1, yes or on. In each case SslConfig.isVerify() returns false and the driver installs a trust-all SSLContext. An attacker on the network path to the Vault server can then read the Vault token and secrets in transit and forge responses. This issue affects io.github.jopenlibs:vault-java-driver 5.2.0 through 6.2.3. It is fixed in 7.0.0.	7.4	More Details
CVE-2026-90634	An uncontrolled memory access in the PDF import code of Apache OpenOffice versions through 4.1.16 allows a crafted PDF to cause an out-of-bounds memory write, causing program crash or memory corruption. Users are recommended to upgrade to version 4.1.17, which fixes this issue.	7.3	More Details
CVE-2026-59268	An out-of-bounds Write vulnerability in Apache OpenOffice versions through 4.1.16 could allow an attacker to craft a Microsoft Word document that would crash the program, or otherwise corrupt other memory areas. Users are recommended to upgrade to version 4.1.17, which fixes this issue.	7.3	More Details
CVE-2026-123963	A security vulnerability has been detected in OpenBMB Internet of Agents up to 9d78e88e47160eb42ee1ee8538c05e1c2c47877a. The impacted element is the function register of the file im_server/app.py of the component Agent Registry. Such manipulation of the argument desc/name leads to missing authentication. 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. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-90628	An uncontrolled memory access in the PDF export code of Apache OpenOffice versions through 4.1.16 allows a crafted CFF font to cause a stack overflow problem, causing program crash or memory corruption, or even running other code. Users are recommended to upgrade to version 4.1.17, which fixes this issue.	7.3	More Details
CVE-2026-123022	A vulnerability was detected in agentscope-ai AgentScope up to 2.0.11. The impacted element is the function subprocess.Popen of the file src/agentscope/mcp/_config.py of the component MCP Workspace API. The manipulation of the argument command results in os command injection. The attack may be launched remotely. The exploit is now public and may be used. The pull request to fix this issue awaits acceptance.	7.3	More Details
CVE-2026-	A flaw has been found in agentscope-ai AgentScope up to 2.0.8. This affects the function check_permissions of the file src/agentscope/tool/_builtin/_bash.py of the component Bash Tool. This manipulation causes incorrect authorization. Remote exploitation of the attack is possible. The exploit has been published and may be used.	7.3	More Details

123023	Upgrading to version 2.0.9 mitigates this issue. Patch name: 6b43b13a46401e86abd3defeed9a8bfe5b37bc6d. It is recommended to upgrade the affected component.		
CVE-2026-123024	A vulnerability has been found in agentscope-ai AgentScope up to 2.0.11. This impacts the function get_current_user_id of the file src/agentscope/app/deps.py of the component Agent Service. Such manipulation of the argument X-User-ID leads to missing authentication. The attack can be executed remotely. The exploit has been disclosed to the public and may be used. The pull request to fix this issue awaits acceptance.	7.3	More Details
CVE-2026-123028	A vulnerability was identified in itsourcecode Online Book Store 1.0. Affected by this issue is some unknown functionality of the file /admin_edit.php. The manipulation of the argument bookisbn with the input 1%27%20AND%20GTID_SUBSET(CONCAT(0x71717a6b71,(SELECT%20(ELT(6040=6040,1))),0x716b6a7171),6040)--%20LpDt as part of String leads to sql injection. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2026-122009	A flaw has been found in DataLinkDC Dinky up to 1.2.5. This vulnerability affects the function FlinkWebURITemplateProxyServlet.getNewTargetUri of the file dinky-admin/src/main/java/org/dinky/utils/FlinkWebURITemplateProxyServlet.java of the component flink_web Proxy Endpoint. This manipulation of the argument _authority causes server-side request forgery. The attack can be initiated remotely. The exploit has been published and may be used. The researcher claims to have submitted a GHSA on the repository of the project.	7.3	More Details
CVE-2026-122019	A vulnerability was identified in 6amTech 6valley 16.0. Impacted is the function existingAccountCheck of the file /api/v1/auth/existing-account-check of the component Social Login Flow. Such manipulation of the argument user_response leads to authorization bypass. The attack may be launched remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2026-90629	An uncontrolled memory access in the WMF import code of Apache OpenOffice versions through 4.1.16 allows a crafted WMF file to cause an invalid memory access, causing program crash or memory corruption. Users are recommended to upgrade to version 4.1.17, which fixes this issue.	7.3	More Details
CVE-2026-92887	Incorrect default value in the REST API framework's .rest.xml definition parser (ModelApiReader) in Apache OFBiz through 24.09.07 on all platforms allows a remote, unauthenticated attacker to invoke a REST API operation without providing valid credentials via a .rest.xml resource or operation definition that omits the auth attribute, which ModelApiReader incorrectly resolves to false instead of the true default declared by rest-api.xsd. Users are recommended to upgrade to version 24.09.08, which fixes this issue.	7.3	More Details
CVE-2026-90624	An unchecked memory access in the PDF import code of Apache OpenOffice versions through 4.1.16 on allows a crafted PDF to execute an out-of-bounds memory write. This could crash the program or cause memory corruption. Users are recommended to upgrade to version 4.1.17, which fixes this issue.	7.3	More Details
CVE-2026-121926	A vulnerability was detected in yezhihao jt808-server up to a07f68c466b560b97ef41edb8a4966469abdf83e. Affected is the function WebMvcConfig.addInterceptors of the component Web Management API. The manipulation results in missing authentication. 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 vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-90626	An uncontrolled memory access in the PDF import code of Apache OpenOffice versions through 4.1.16 allows a crafted PDF to cause an out-of-bounds memory write, causing program crash or memory corruption. Users are recommended to upgrade to version 4.1.17, which fixes this issue.	7.3	More Details
CVE-2026-123881	A vulnerability was found in OpenBMB Internet of Agents up to 9d78e88e47160eb42ee1ee8538c05e1c2c47877a. This issue affects the function fetch_chat_record of the file im_server/app.py of the component Message Handler. The manipulation of the argument comm_id results in improper access controls. The attack may be performed from remote. The exploit has been made public and could be used. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-104656	Improper neutralization of input in the sessions grid in Progress Telerik Fiddler Everywhere 8.3.0 and earlier allows an attacker to execute backend IPC commands by convincing a user to open a specially crafted SAZ file.	7.3	More Details
CVE-2026-123019	A weakness has been identified in eosphoros-ai DB-GPT up to 0.8.2. Impacted is the function exec_module of the file hf_adapter.py of the component HuggingFace Adapter. Executing a manipulation of the argument trust_remote_code can lead to inclusion of functionality from untrusted control sphere. The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-123032	A security flaw has been discovered in OpenBMB Internet of Agents up to 9d78e88e47160eb42ee1ee8538c05e1c2c47877a. This affects the function ConnectionManager.connect of the file im_server/app.py of the component WebSocket Connection Manager. The manipulation of the argument agent_name results in missing authentication. 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-2026-122050	A vulnerability was found in Campcodes Complete Sales and Inventory System with Credit Management 1.0. This issue affects some unknown processing of the file /ahira/login.php. Performing a manipulation of the argument branch results in sql injection. The attack is possible to be carried out remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2026-121009	SQL::Abstract versions from 1.90_01 before 2.000001_04 for Perl skip the injection_guard check for function names given with -func. injection_guard is documented to apply to every function name, but only the { -name => ... } shorthand goes through it. The explicit { -func => [$name, ...] } form puts $name into the SQL unchecked. An application that relies on injection_guard to reject an untrusted function name passed with -func allows SQL injection.	7.3	More Details
CVE-2026-69005	Integer overflow in NPU driver parameter processing due to insufficient bounds checking.	7.3	More Details
CVE-2026-123791	A vulnerability was detected in OpenBMB Internet of Agents up to 9d78e88e47160eb42ee1ee8538c05e1c2c47877a. This affects the function _primary_field_query of the file common/utils/milvus_utils.py of the component Agent Registry. The manipulation of the argument key results in improper neutralization of special elements in data query logic. 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.	7.3	More Details
CVE-2026-122048	A vulnerability was identified in Campcodes Division Regional Athletic Meet Game Result Matrix System up to 2.1. This affects an unknown function of the file /dipam/check-user.php. Such manipulation of the argument abbr leads to sql injection. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2026-122047	A security vulnerability has been detected in Campcodes Complete Advance Loan Management System 1.0. This affects the function move_uploaded_file of the file /loan/application/banner.php. Such manipulation of the argument image leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2026-121007	SQL::Abstract versions from 1.90_01 before 2.000001_04 for Perl allow SQL injection via the where values of a nested statement in an identifier position. A nested statement such as { -select => ... } in a position where plain scalars are identifiers treats its own plain scalars as identifiers too. These positions are the select list, ORDER BY, GROUP BY, RETURNING, and with the ExtraClauses plugin FROM (-as) and JOIN (to). The values of the statement's where, having and set clauses, and the rows of a -values, go into the SQL text instead of the bind list, unescaped unless quote_char is set. Subselects in a WHERE condition are not affected. An application that passes untrusted input as a where value of such a nested statement, expecting it to be bound, allows SQL injection.	7.3	More Details
CVE-2026-122038	A vulnerability was identified in krupalshah EmployeeRecruitmentSystem up to 922ff6d208278282e7c8e36d70d9ae356adec9fe. Affected by this issue is the function mysql_query of the file source/reqformprocessing.php of the component Requirement Board Update Handler. Such manipulation leads to sql injection. The attack can be launched remotely. The exploit is publicly available and might be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The vendor was contacted early about this disclosure but did not respond in any way. This vulnerability only affects products that are no longer supported by the maintainer.	7.3	More Details
CVE-2026-121610	A security flaw has been discovered in funadmin 7.1.0. Impacted is the function Curd::selectList of the file /frontend/ajax/index of the component Frontend List Endpoint. The manipulation of the argument selectFields results in sql injection. The attack can be executed 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-2026-68994	A double free vulnerability in NPU driver due to improper pointer management (941)	7.3	More Details
CVE-2026-121608	A vulnerability was determined in Qihoo 360 D603-2, D600-2 and D606-6 up to 6.3.2. This vulnerability affects the function on_push_message of the file /fs2/bin/iscm of the component Timezone Push Handler. Executing a manipulation of the argument tz can lead to os command injection. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized. Upgrading to version 6.4.0 is able to resolve this issue. Upgrading the affected component is advised. Firmware 6.4.0 gates the path with a new check_timezone_parameter validation (verified by VulDB vulnerability analysis team via disassembly).	7.3	More Details
CVE-2026-122037	The AgenWebsite Shipping – Plugin Ongkos Kirim & Generate Resi Otomatis Semua Kurir Indonesia plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'zipcode' parameter in all versions up to, and including, 9.2.41 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-	CGI versions before 5.00 for Perl allow HTTP header injection via entity decoding after the newline check in header and unchecked values in multipart_start and do_push. With autoEscape off, header decodes HTML entities in extra header values after its newline check, so an encoded CR or LF reaches the response. multipart_start does	7.2	More

120639	not check header values for newlines, and do_push does not check the type it prints in each part. An application that passes request data into these header values can be made to add headers or split the response.		Details
CVE-2026-116537	The Link Library plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'link_description' parameter in all versions up to, and including, 7.10.0 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 exploit requires the site administrator to have enabled the non-default 'Convert [] to <> in Link Description and Notes' (use_html_tags) setting; when this option is off, the bracket-to-angle-bracket conversion never runs and the payload is never reconstructed into executable HTML.	7.2	More Details
CVE-2026-111370	The WP Visitor Statistics (Real Time Traffic) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'os (also browser, res)' parameter in all versions up to, and including, 8.9.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2026-120082	The GeoDirectory – WP Business Directory Plugin and Classified Listings Directory plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'post_content' parameter in all versions up to, and including, 2.8.200 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 nested shortcode payload ([gd_dynamic_conten[gd_tags]t ...]) defeats the plugin's geodir_strip_shortcodes() guard because WordPress's strip_shortcodes() performs only a single pass over registered tags, and HTML-entity-encoded attributes in the resulting shortcode survive wp_kses_post() because kses inspects HTML tags rather than shortcode attribute values.	7.2	More Details
CVE-2026-116558	The Unlimited Elements for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the '<title>/<description> inside the attacker-controlled RSS feed body' parameter in all versions up to, and including, 2.0.26 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 against any site whose administrator has placed the RSS Feed catalog widget pointing at a feed URL the attacker controls, as the plugin's own 2.0.25 escaping pre-processor intentionally excludes |raw prints in element content positions from its escaping logic, and XML entity-encoded payloads in feed item titles are decoded back to raw markup before reaching the sink.	7.2	More Details
CVE-2026-120512	The Form Maker by 10Web – Mobile-Friendly Drag & Drop Contact Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'wdform_<n>_element<id> (Hidden Input field, name = user-defined, e.g. hidden_probe)' parameter in all versions up to, and including, 1.15.50 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 open the Submissions screen and click the Show-on-Map link associated with the poisoned entry, at which point the attacker-controlled field_id value is echoed unescaped into a single-quoted JavaScript string in the FormMakerEditCountryinPopup popup — a step whose nonce and capability checks are automatically satisfied by the administrator's own session and the freshly minted fm_ajax_nonce embedded in the link.	7.2	More Details
CVE-2026-97397	The Remove Google Fonts – Disable, Block, or Replace with Bunny Fonts for GDPR Compliance plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Comment Field via Regex-Mangled Output Buffer in all versions up to, and including, 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. Successful exploitation requires the plugin's Remove mode to be active and the malicious comment to be published, either through auto-approval for known commenters or manual moderator approval.	7.2	More Details
CVE-2026-121946	zbateson mail-mime-parser before 3.0.9 and 4.x before 4.0.6 contains a CRLF header injection vulnerability in message-building helpers that fail to strip CR and LF characters. Attackers supplying crafted MIME type, charset, encoding, micalg, or protocol values can inject extra header lines such as a forged Bcc into outgoing messages.	7.2	More Details
CVE-2025-11229	The system fails to properly enforce scope authorization when the `authorize_all_scopes` configuration is enabled. This allows applications using the client credentials grant type to obtain all API scopes, including sensitive internal and console scopes, without requiring explicit authorization, bypassing intended access controls. Exploitation of this vulnerability can lead to privilege escalation, enabling unprivileged clients to perform unauthorized administrative actions, access confidential organizational data, and potentially achieve full account takeover in deployments where the `authorize_all_scopes` configuration deviates from its default disabled state.	7.2	More Details
CVE-2026-123010	@twilio-labs/netlify-okta-auth through 1.0.2 relies on an unverified iss claim. This affects an outbound HTTP request to retrieve a public signing key. There may be other impacts in a misconfiguration where oktaUrl isn't set.	7.2	More Details
CVE-2026-115498	The Slim Jetpack plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'g<PAGE_ID>-website (Website contact-field)' parameter in all versions up to, and including, 2.7.0.1 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. The nonce and authentication checks on form submission are only enforced for logged-in users, allowing unauthenticated visitors to store payloads via any page containing the [contact-form] shortcode.	7.2	More Details
	The Happyforms plugin for WordPress is vulnerable to Stored Cross-Site Scripting via spoofable client IP headers in versions up to, and including, 1.38.9. This is due to the happyforms_get_client_ip() function reading raw		

CVE-2026-93755	HTTP_CLIENT_IP and HTTP_X_FORWARDED_FOR request headers without any validation or sanitization, storing the value as post meta ('client_ip') via update_post_meta() during unauthenticated form submissions, and later echoing it in the admin submission edit screen's Details metabox without output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user (typically an administrator reviewing a submission) accesses an injected page.	7.2	More Details
CVE-2026-120540	The iubenda | All-in-one Compliance for GDPR / CCPA Cookie Consent + more plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to, and including, 3.13.6. This is due to the way iubendaParser::parse_comments() re-processes HTML inside IUB-COOKIE-BLOCK markers through the bundled simple_html_dom parser after WordPress has already KSES-filtered the saved comment: simple_html_dom's remove_noise() stores <code> bodies under a deterministic key ('___noise___ 1000') and restore_noise() later substitutes any matching substring back into attribute values WITHOUT re-escaping, allowing a quote-breaking payload stashed in an allowed <code> element to be injected into an allowed <abbr title="___noise___ 1000"> attribute at render time. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page, after an administrator approves the first (otherwise moderated) comment under WordPress's default comment_previously_approved setting.	7.2	More Details
CVE-2026-115811	The Strong Testimonials plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'star_rating' parameter in all versions up to, and including, 3.3.16 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. Successful execution requires an administrator to open the standard Preview link for a pending testimonial, a step the plugin's normal moderation workflow naturally invites.	7.2	More Details
CVE-2026-110776	The MDTF – Meta Data and Taxonomies Filter plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'vars' parameter in all versions up to, and including, 1.4.1 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. This requires that a published page or post on the target site contains the [meta_data_filter_results] shortcode, which is the primary output feature of the plugin.	7.2	More Details
CVE-2026-63213	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to 7.15.2 and 8.10.2, the Upgrade Wizard commit flow trusts the hidden zip_to_dir parameter, while clean_path() does not reject traversal sequences. An authenticated administrator can copy extracted package files outside the intended destination, overwrite application or configuration files, place executable PHP under the web root, or cause denial of service. This issue is fixed in versions 7.15.2 and 8.10.2.	7.2	More Details
CVE-2026-109214	The User Frontend – Membership, User Registration, User Profile, User Directory & Content Restriction with Frontend Post Submission plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the '<taxonomy_field_name> (default: 'category')' parameter in all versions up to, and including, 4.3.13 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Exploitation requires the target installation to have configured a Taxonomy field in text-input mode with guest post submission enabled on at least one frontend form.	7.2	More Details
CVE-2026-17401	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to execute arbitrary code due to a stack-based buffer overflow.	7.2	More Details
CVE-2026-110291	The Graphina – Charts and Graphs For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'iq_tree_chart_node_font_family (and any text control serialized into chart_data['settings'])' parameter in all versions up to, and including, 3.1.13 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Elementor's Utils::kses_post_deep() does not strip the attack payload on save because the payload contains no disallowed HTML tags — only a single quote and an event-handler fragment — allowing the malicious value to survive persistence.	7.2	More Details
CVE-2026-109230	The WP Visitor Statistics (Real Time Traffic) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'browser' parameter in all versions up to, and including, 8.7.1 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. The payload is stored via an unauthenticated HTTP request to the public visitor tracking endpoint (wmcAction=wmcTrack) and executes when the bundled jqPlot PieRenderer inserts the HTML-decoded series label directly as HTML in the authenticated administrator's browser.	7.2	More Details
CVE-2026-17341	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote attacker to perform server-side request forgery and relay unauthorized email messages due to improper neutralization of user-supplied input.	7.2	More Details
CVE-2026-93766	The Happyforms Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'happyforms_client_referer' parameter in all versions up to, and including, 1.38.9 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-	The VikBooking Hotel Booking Engine & PMS plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'guests[][][documents]' Parameter in all versions up to, and including, 1.8.17 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages		More

2026-93429	that will execute whenever a user accesses an injected page. This requires the attacker to possess a valid booking sid/ts pair, which can be obtained by making a standard public booking, as the session token needed to satisfy the JSession::checkToken() gate is emitted in the publicly accessible pre-checkin form.	7.2	Details
CVE-2026-120739	The Optimole – Optimize Images | Convert WebP & AVIF | CDN & Lazy Load | Image Optimization plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 's (missing_srcsets[*][*].s)' parameter in all versions up to, and including, 4.2.18 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. The HMAC signature required to pass the REST endpoint's authorization check is published in plaintext to unauthenticated visitors inside the inline optimoleDataOptimizer JavaScript object on any page with an incomplete profile, making the effective authentication barrier nonexistent.	7.2	More Details
CVE-2026-119070	The Optimole – Optimize Images | Convert WebP & AVIF | CDN & Lazy Load | Image Optimization plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'comment' parameter in all versions up to, and including, 4.2.17 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The exploit requires the plugin to be in its normal connected state (cdn_key and cdn_secret configured) with the image replacer enabled, which is the default post-setup configuration; the stored payload bypasses all WordPress comment sanitization filters because it contains no HTML metacharacters at storage time — the characters are produced only by Optimole's own decoder at render time.	7.2	More Details
CVE-2026-87964	The Product Feed Manager for WooCommerce – CTX Feed – Support 220+ Shopping, AI & Social Channels plugin for WordPress is vulnerable to PHP Code Injection in all versions up to, and including, 8.0.26. This is due to insufficient sanitization of the `feedConfigCustom2` parameter — only `wp_unslash()` is applied before the value is stored verbatim via `update_option()`, and during feed generation the `Custom2Template::evaluate_return()` method passes the stored `{(return ...)}` template expressions directly to PHP's `eval()` function without any code-level sanitization. This makes it possible for authenticated attackers, with Shop Manager-level access and above, to inject and execute arbitrary PHP code on the server, escalating their privileges beyond what the role normally permits to full remote code execution and site takeover. The `ctxfeed_custom2_eval_enabled` option defaults to `true`, meaning no additional administrator configuration is required for this attack path to be exploitable out of the box.	7.2	More Details
CVE-2026-119183	The JetFormBuilder — Dynamic Blocks Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the '<form field mapped to a post meta key, e.g. lst_cost>' parameter in all versions up to, and including, 3.6.8 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. Exploitation requires the target site to have configured a public Insert Post form writing to a post meta key and a Calculated Field whose formula references that key via the %META::key% macro, after which a single unauthenticated POST is sufficient to persist the payload.	7.2	More Details
CVE-2026-123418	The Church Admin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'lat' 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. This vulnerability is only exploitable when a Google Maps API key has been configured in Church Admin settings, as the vulnerable sink is only reached when that option is present.	7.2	More Details
CVE-2026-39431	On HP Poly EagleEye Cube USB 1.3.1-001267 devices, one of the API functions available on a management service accessible via USB allows command injection. This allows attackers (without administrator-level access) to execute arbitrary commands on the device as root. This is due to insufficient input validation that allows an attacker to control part of the CSR certificate generation process. This provides full root access that permits full control over device operations, unauthorized access to data, and the ability to place a persistent backdoor on the device (which could operate via the Ethernet port).	7.2	More Details
CVE-2026-120537	The TranslatePress – Translate Multilingual sites with AI Translation plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'comment (storage); originals / language / original_language (exfiltration from endpoint)' parameter in all versions up to, and including, 3.3.8 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2026-119175	The Flying Images: Optimize and Lazy Load Images for Faster Page Speed plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'comment' parameter in all versions up to, and including, 2.4.15 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. A first-time commenter's submission requires a single administrator approval under the default comment_previously_approved setting; however, once approved, all subsequent comments from the same name and email pair bypass moderation, and the injected script executes for every visitor — including administrators viewing the post from the front end.	7.2	More Details
CVE-2026-119167	The TranslatePress – Translate Multilingual sites with AI Translation plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'comment' parameter in all versions up to, and including, 3.3.8 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. Successful exploitation requires that at least one prior comment from the attacker's name and email pair has been approved under	7.2	More Details

	WordPress's default comment_previously_approved moderation setting, and that a secondary language is configured in TranslatePress.		
CVE-2026-75590	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote attacker to access internal network resources and obtain sensitive information due to server-side request forgery. A protection that blocks requests to internal addresses can be bypassed, so the server could be made to contact internal services and return part of their responses.	7.2	More Details
CVE-2026-111317	The JetFormBuilder — Dynamic Blocks Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the '<any form field name — e.g. 'payload'>' parameter in all versions up to, and including, 3.6.7 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. Exploitation requires the targeted form to have both the Save Form Record action enabled and a form-level Form Record preset configured; the stored payload only executes when a privileged user visits the front-end form page with the preset's record query variable set to the attacker's submitted record ID.	7.2	More Details
CVE-2026-115548	The Quttera ThreatSign – Web Malware Scanner for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'HTTP_USER_AGENT' parameter in all versions up to, and including, 4.1.0.48 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 an administrator accesses an injected page.	7.2	More Details
CVE-2026-120677	The Optimole – Optimize Images | Convert WebP & AVIF | CDN & Lazy Load | Image Optimization plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'comment' parameter in all versions up to, and including, 4.2.18 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 the comment to be approved by an administrator and for the affected post to contain at least one iframe or video element (e.g., a core Video block), which is sufficient under default plugin settings where video lazy loading is enabled.	7.2	More Details
CVE-2026-119158	The Pie Register – User Registration, Profiles & Content Restriction plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'first_name' parameter in all versions up to, and including, 3.8.4.16 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 is exploitable when public registration is enabled and the registration form includes a Profile Picture field; the attacker registers via the publicly accessible form (nonce is emitted to unauthenticated visitors) to store the payload, then logs in as the newly created Subscriber to post a comment that triggers delivery to all page visitors.	7.2	More Details
CVE-2026-17316	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote attacker to perform server-side request forgery due to improper validation of user-supplied input.	7.2	More Details
CVE-2026-119156	The Download Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'wpdm_reg[first_name], wpdm_reg[last_name], wpdm_reg[user_login]' parameter in all versions up to, and including, 7.5.9 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 to have "Anyone can register" enabled, the plugin's [wpdm_reg_form] shortcode published on a public page, and at least one package authored by user ID 1 rendered with the Spotlight link template.	7.2	More Details
CVE-2026-122231	The WS Form LITE – Drag & Drop Contact Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'field_<id>[0][0]' parameter in all versions up to, and including, 1.12.18 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. This is possible because the client-side esc_html() helper returns any non-string value unchanged, allowing a nested-array payload coerced via Array.prototype.toString to reach jQuery .append() unescaped.	7.2	More Details
CVE-2026-119747	The GetPaid plugin for WordPress before 2.8.63 contains an incorrect authorization vulnerability where the check_post_permissions() method in includes/api/class-getpaid-rest-posts-controller.php maps REST operations to generic WordPress post capabilities instead of enforcing the plugin's manage_invoicing permission. Authenticated users with lower-privileged roles such as Editor or Author can exploit this flaw to list other users' invoices, mark pending invoices as paid without recording payment transactions, or create published items and new invoices through the REST API.	7.1	More Details
CVE-2026-103938	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to 8.3.0, interface/patient_file/pos_checkout_ippf.php performs state-changing void, voidall, and regen operations through GET requests without CSRF token validation. The form_checksum integrity check is conditional and is skipped when the parameter is omitted, allowing a cross-site request to force an authenticated billing user to void checkouts or regenerate invoice counters. The resulting changes can alter ledger state, financial reporting, and audit records. This issue is fixed in version 8.3.0.	7.1	More Details
CVE-2026-	FreeScout is a self-hosted help desk and shared mailbox. Prior to 1.8.231, the profile form exposes the only_assigned_tickets permission to its non-admin owner, and UsersController::profileSave() adds or removes User::PERM_ONLY_ASSIGNED_TICKETS without checking that the editor is an administrator. A restricted agent can uncheck the option, or submit an ordinary profile save that omits it, to remove the administrator-imposed	7.1	More Details

103985	restriction. The agent can then read and modify conversations assigned to other agents in every mailbox they already belong to. This issue is fixed in version 1.8.231.		
CVE-2026-18142	IBM MQ 9.2.0.0 through 9.2.0.44 LTS, 9.3.0.0 through 9.3.0.42 LTS, 9.4.0.0 through 9.4.0.26 LTS, 9.4.0.0 through 9.4.5.1 CD, and 10.0.0.0 through 10.0.0.5 LTS and CD could allow a remote authenticated attacker to cause a denial of service and perform limited memory corruption due to an integer overflow.	7.1	More Details
CVE-2026-123489	Craft CMS 4.0.0 before 4.18.9 and 5.0.0 before 5.11.2 contains a blind SQL injection vulnerability because the sandbox-exposed getNext() and getPrev() methods pass arbitrary criteria arrays to Craft::configure() without removing SQL-bearing properties such as orderBy and where. Authenticated control panel users can supply a crafted elementIds value, rendered as a sandboxed template, to obtain a conditional SQL oracle under the Craft database account.	7.1	More Details
CVE-2026-39744	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WC Lovers WCFM Membership wc-multivendor-membership allows Stored XSS.This issue affects WCFM Membership: from n/a through 2.12.0.	7.1	More Details
CVE-2026-109883	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Elementor Elementor Website Builder elementor allows Code Injection.This issue affects Elementor Website Builder: from n/a through 4.3.5.	7.1	More Details
CVE-2026-13284	IBM MQ 9.2.0.0 through 9.2.0.44 LTS, 9.3.0.0 through 9.3.0.42 LTS, 9.4.0.0 through 9.4.0.26 LTS, 9.4.0.0 through 9.4.5.1 CD, and 10.0.0.0 through 10.0.0.5 LTS and CD is vulnerable to an XML external entity injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources.	7.1	More Details
CVE-2026-87008	Code Graph RAG is an AI-powered knowledge graph and retrieval system for querying, understanding, and editing multi-language codebases. Prior to 0.0.589, AstGrepService in codebase_rag/tools/ast_grep_service.py enumerates files beneath project_root and relies on should_skip_path in codebase_rag/utils/path_utils.py to classify them, but the containment check operates on unresolved lexical paths. A symbolic link planted inside an analyzed repository can therefore reference a file outside the configured root while still appearing in scope. The structural_search tool follows the link and discloses readable content without an approval gate, while structural_replace with dry_run=False follows it and overwrites writable content; the MCP path invokes structural replacement without the agent-loop approval control. An attacker who causes a victim to analyze a repository containing such a link can read credentials, keys, environment files, or sibling source and can modify files accessible to the code-graph-rag process. This issue is fixed in version 0.0.589.	7.1	More Details
CVE-2026-13289	IBM MQ 9.2.0.0 through 9.2.0.44 LTS, 9.3.0.0 through 9.3.0.42 LTS, 9.4.0.0 through 9.4.0.26 LTS, 9.4.0.0 through 9.4.5.1 CD, and 10.0.0.0 through 10.0.0.5 LTS and CD is vulnerable to an XML external entity injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources.	7.1	More Details
CVE-2026-62007	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 2.0.26.	7.1	More Details
CVE-2026-121765	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 3.3.8.	7.1	More Details
CVE-2026-123326	In JetBrains YouTrack before 2026.2.19197 incorrect authorisation in the scripts debugger allowed workflow script disclosure and suspension	7.1	More Details
CVE-2026-104133	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to 8.3.0, interface/modules/custom_modules/oe-module-dorn/public/compendium_install.php checks authentication and CSRF but does not require the admin/users ACL enforced by sibling DORN administration scripts. When the DORN module is enabled, a low-privilege authenticated user can supply a labGuid that causes LabCompendiumInstall::uninstall() to delete detail and result procedure types and deactivate order types before the reinstall step. The action can corrupt lab-ordering configuration and require an administrator to restore the compendium. This issue is fixed in version 8.3.0.	7.1	More Details
CVE-2026-97847	A flaw was found in the protocol mapper and identity resolution components of Keycloak. The issue occurs when a client manager uses hardcoded-claim mappers to override identity claims in sessionless service-account tokens. Because these tokens lack a session ID, Keycloak may incorrectly resolve the token bearer as a different, highly privileged user based on the manipulated claims. This can allow an attacker with limited client management permissions to impersonate a realm administrator and gain full control over the realm.	7.1	More Details
CVE-2026-54851	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Awesomemotive Contact Form by WPForms wpforms-lite allows Reflected XSS.This issue affects Contact Form by WPForms: from n/a through 2.0.3.	7.1	More Details
CVE-	In JetBrains IntelliJ IDEA before 2026.3 arbitrary file write was possible via symlinks when extracting plugin		More

2026-123842	archives	7.1	Details
CVE-2026-17322	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a local attacker to obtain sensitive credentials and compromise accounts due to insertion of sensitive information into log files.	7.1	More Details
CVE-2026-119366	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AdvancedCoding wpDiscuz wpdiscuz allows Stored XSS.This issue affects wpDiscuz: from n/a through 7.6.73.	7.1	More Details
CVE-2026-100361	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to 7.15.2 and 8.10.2, the V8 write path checks that a field exists but does not enforce api-visible or sensitive metadata that hides the same field on reads. The affected flow begins at PATCH /Api/V8/module and uses user_hash, external_auth_only, api-visible: false, and sensitive: true to carry attacker-controlled data or authorization state into the security-sensitive operation. An authenticated user can mass-assign internal authentication fields, modify password hashes or external-authentication flags, and persist unauthorized account access. This issue is fixed in versions 7.15.2 and 8.10.2.	7.1	More Details
CVE-2026-17319	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to modify tool configuration and cause a denial of service due to improper authorization. Information supplied by the client is relied on when deciding what a user is allowed to do, which could allow unauthorized changes that disrupt service.	7.1	More Details
CVE-2026-102664	ProxySQL is a proxy for MySQL and its forks, as well as PostgreSQL. Prior to 3.0.10, 3.1.10, and 4.0.10, decompress_mysql_payload() in lib/mysql_data_stream.cpp accepts a zlib stream when uncompress() returns Z_OK without checking that the actual output length equals the attacker-controlled payload_length. An authenticated MySQL client that negotiates compression can overstate payload_length, causing buffer2array() to parse the uninitialized tail of a heap buffer as MySQL packet headers and forward stale data to the backend. Backend error responses can disclose prior SQL queries, result data, credentials, or session state, and malformed lengths can also cause excessive allocations. This issue is fixed in versions 3.0.10, 3.1.10, and 4.0.10.	7.1	More Details
CVE-2026-100364	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to 7.15.2 and 8.10.2, the V8 JSON:API update path fails to remove the id attribute before assigning user-supplied attributes to a SugarBean. The affected flow begins at updateRecord() and uses processAttributes(), id, and ACL_ALLOW_OWNER to carry attacker-controlled data or authorization state into the security-sensitive operation. An authenticated user can substitute a victim record identifier, bypass owner-only authorization, overwrite another record, and hijack record ownership. This issue is fixed in versions 7.15.2 and 8.10.2.	7.1	More Details
CVE-2026-123325	In JetBrains YouTrack before 2025.3.170763, 2026.1.14150, 2026.2.19656 inclusion of untrusted remote code was possible via the plugin sandbox page	7.1	More Details
CVE-2026-17311	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to modify application API subscriptions due to broken object-level authorization.	7.1	More Details
CVE-2026-109884	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Elementor Elementor Website Builder elementor allows Reflected XSS.This issue affects Elementor Website Builder: from n/a through 4.3.5.	7.1	More Details
CVE-2026-108041	The SEOPress WordPress plugin before 10.4 does not sanitise and escape some of its analytics tracking settings before outputting them in an inline script printed on every front-end page, allowing users granted a SEOPress WordPress plugin before 10.4 capability that an administrator can delegate to lower-privileged roles to perform Stored Cross-Site Scripting attacks that execute in the browser of any site visitor, including a logged-in administrator viewing the front end.	7.1	More Details
CVE-2026-119477	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jacob N. Breetvelt WP Photo Album Plus wp-photo-album-plus allows Stored XSS.This issue affects WP Photo Album Plus: from n/a through 9.3.05.003.	7.1	More Details
CVE-2026-54861	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Aguila Technologies WP Customer Area customer-area allows Reflected XSS.This issue affects WP Customer Area: from n/a through 8.4.1.	7.1	More Details
CVE-2026-69136	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to 7.15.2 and 8.10.2, email template attachment handling passes the remove_attachment POST parameter array through HTML-oriented securexss() processing and directly interpolates its elements into an SQL UPDATE statement. An authenticated attacker can inject SQL to disclose database information or abuse the UPDATE context to soft-delete all records in the notes table in one request. This issue is fixed in versions 7.15.2 and 8.10.2.	7.1	More Details
CVE-2026-69135	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to 7.15.2 and 8.10.2, the Project module interpolates the authenticated caller's duplicateId POST parameter directly into a SQL query without sanitization, quoting, or parameterization. An authenticated attacker can alter	7.1	More Details

	query structure and disclose sensitive database information. This issue is fixed in versions 7.15.2 and 8.10.2.		
CVE-2026-57639	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Roland Murg WP Booking System wp-booking-system allows Reflected XSS.This issue affects WP Booking System: from n/a through 2.1.0.6.	7.1	More Details
CVE-2026-57666	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Aguila Technologies WP Customer Area customer-area allows Reflected XSS.This issue affects WP Customer Area: from n/a through 8.4.1.	7.1	More Details
CVE-2026-82916	Missing Authorization in XmlDsDump in Apache OFBiz 24.09 before 24.09.08 on all platforms allows a remote authenticated attacker holding only the webtools base permissions (OFBTOOLS_VIEW, WEBTOOLS_VIEW) — explicitly not the ENTITY_MAINT permission the export feature declares and visibly refuses to render for — to export the contents of any database entity, including UserLogin with its currentPassword hashes, to any filesystem path the OFBiz process can write, including a web-served docroot, and to create arbitrary directories or truncate arbitrary existing files at those paths, because the XmlDsDump screen action writes the requested entity data via new FileOutputStream on unvalidated outpath and filename request parameters before the screen's ENTITY_MAINT permission check runs, unlike the equivalent Java service entityExportAll, which enforces both a permission check and a file-path allow-list. Users are recommended to upgrade to version 24.09.08, which fixes this issue.	7.1	More Details
CVE-2026-119488	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Shamim Rajani Pie Register pie-register allows Stored XSS.This issue affects Pie Register: from n/a through 3.8.4.15.	7.1	More Details
CVE-2026-113782	ESP-IDF is the Espressif Internet of Things (IOT) Development Framework. From 5.2.0 until 5.2.8, 5.3.6, 5.4.5, 5.5.5, and 6.0.3, the OpenThread Border Router Neighbor Discovery packet handler trusts an attacker-controlled ICMPv6 option length while copying into a fixed stack buffer. A host on the same infrastructure link as the Border Router can send a crafted ICMPv6 Router Advertisement to its infrastructure interface whose oversized length causes an out-of-bounds write into adjacent stack memory. Firmware is affected only when CONFIG_OPENTHREAD_BORDER_ROUTER=y; Thread end devices, routers, and RCP firmware without the Border Router feature are unaffected. Exploitation requires no authentication or user interaction and can crash or reboot the device or corrupt adjacent stack state. This issue is fixed in versions 5.2.8, 5.3.6, 5.5.5, and 6.0.3 and is scheduled to be fixed in version 5.4.5.	7.1	More Details
CVE-2026-115431	Missing Authorization vulnerability in WP Swings Upsell Order Bump Offer for WooCommerce upsell-order-bump-offer-for-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Upsell Order Bump Offer for WooCommerce: from n/a through 3.1.6.	7.1	More Details
CVE-2026-109150	The WP PageNavi Style WordPress plugin through 1.4 does not sanitise and escape some of its settings, and has no CSRF check when they are saved, which could allow attackers to make a logged-in administrator store arbitrary JavaScript via a CSRF attack that is then executed in the browser of everyone who visits the site's front end.	7.1	More Details
CVE-2026-118422	The Stape Conversion Tracking WordPress plugin before 2.3.11 does not validate the sub-path appended to its same-origin proxy's upstream endpoint, allowing unauthenticated visitors to redirect the server-side request to an arbitrary host and have the response body and its content type returned from the site's own origin with security response headers stripped, leading to Server-Side Request Forgery, including loopback and internal hosts, and Cross-Site Scripting.	7.1	More Details
CVE-2026-17284	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to perform unauthorized operations in other tenants' environments due to improper validation of client-supplied information. Tenant context is not sufficiently verified, which could allow actions on resources belonging to other tenants.	7.1	More Details
CVE-2026-119468	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Noptin Newsletter Team Noptin newsletter-optin-box allows Stored XSS.This issue affects Noptin: from n/a through 4.4.2.	7.1	More Details
CVE-2026-123849	In JetBrains IntelliJ IDEA before 2026.3 code execution was possible in untrusted projects via the Terraform File Watchers	7.0	More Details
CVE-2026-87038	The user-mode verification handler for the i3c_transfer() system call, z_vrfy_i3c_transfer() in drivers/i3c/i3c_handlers.c, validated the caller-supplied struct i3c_device_desc in place instead of snapshotting it. It confirmed only that the descriptor was readable by the calling thread (K_SYSCALL_MEMORY_READ()), read target->bus once to check it with K_SYSCALL_OBJ(), and then passed the caller's live pointer down. The implementation z_impl_i3c_transfer() re-reads target->bus from that user memory and dispatches through it as DEVICE_API_GET(i3c, target->bus)->i3c_xfers(...), so the bus that was validated is not necessarily the bus that is used. DEVICE_API_GET() performs no runtime type check outside CONFIG_DEVICE_API_ASSERT builds. On a build with CONFIG_USERSPACE and an I3C controller driver, a user thread that has been granted an I3C device object can exploit this with a second thread in the same memory domain: one thread calls i3c_transfer() while the other rewrites the bus field of the descriptor. The window between the check and the use spans the num_msgs validation, the message-array access check, a stack VLA allocation and a memcpy() of up to 32 struct i3c_msg, so the race is repeatable and can simply be retried until it lands. When the substitution succeeds, the kernel	7.0	More Details

	dereferences an attacker-chosen pointer as a struct device, loads a function pointer from the attacker-controlled api table and calls it in supervisor mode with attacker-influenced arguments. This yields kernel-mode code execution from an unprivileged user thread — a complete escape of the userspace memory-protection sandbox; lesser outcomes are an arbitrary two-level kernel read or a kernel fault. Builds without CONFIG_USERSPACE, or without an I3C driver, are unaffected. The fix copies the descriptor into a kernel-stack local with k_usermode_from_copy(), validates the bus in that copy, and dispatches on the copy, so the validated value is provably the value used.		
CVE-2026-123315	In JetBrains Junie CLI before 26.8.24 command execution was possible via the Allow Similar Commands option	7.0	More Details
CVE-2026-112109	A local privilege escalation vulnerability in Thales SafeNet Authentication Client (SAC) SACSrv can allow an authenticated, non-administrator local user to trigger a heap-based buffer overflow through the service interface. Successful exploitation may allow arbitrary code execution with Local System privileges.This issue affects SAC releases up to and including 10.9 R3 GA (build 10.9.7449).	7.0	More Details
CVE-2026-91168	Warpgate is an open source SSH, HTTPS, and MySQL bastion host for Linux. From 0.21.0 until 0.29.0, the Kubernetes request correlator in warpgate-protocol-kubernetes/src/correlator.rs keys an authorized AdmittedTarget by username, target_name, and client IP rather than by the immutable user UUID, while KubernetesSessionHandle::close does not evict the entry. If an account is deleted and a different low-privilege account is created with the same username, the replacement account can successfully authenticate as that recreated username and reuse the predecessor's still-live correlation entry when requesting the same target from the same client IP before kubernetes.session_max_age expires. Current-request authentication still occurs, but the reused entry bypasses a fresh target authorization check and can cause Warpgate to proxy requests with Kubernetes target credentials that the replacement account is not authorized to use, exposing cluster resources or permitting unauthorized mutations. This issue is fixed in version 0.29.0.	6.8	More Details
CVE-2026-114427	The GutenKit WordPress plugin before 2.5.5 does not properly sanitize custom CSS saved against a post before printing it inside an inline style block on the published page, allowing users with the Author role and above to break out of the style element and store JavaScript that executes in the browser of any visitor who views the post. Exploitation affects sites running WordPress below 7.0.	6.8	More Details
CVE-2026-17308	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote attacker to obtain sensitive credentials and manipulate tool responses due to improper certificate validation.	6.8	More Details
CVE-2026-118786	Improper input validation in non-secure-callable (NSC) veneer functions of the NXP MCUXpresso SDK rpmsg-lite multicore example (multicore_examples/rpmsg_lite_pingpong_tzm) up to releases 26.06.00-lts and 26.09.00 may allow a non-secure caller to supply unvalidated pointers and size values, potentially resulting in disclosure of secure-world memory to the non-secure domain, or denial of service. All software versions starting from 26.06.01-lts and 26.12.00-pvw1 have fixed this issue.	6.8	More Details
CVE-2026-19124	IBM API Connect 10.0.8.0 through 10.0.8.12 could allow an attacker with access to stored data to decrypt sensitive credentials due to the use of a hard-coded cryptographic key. The key protecting stored credentials is built into the product, so credentials could be decrypted if the stored data is obtained.	6.8	More Details
CVE-2026-105459	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow an attacker to gain unauthorized access to an organization due to improper verification of a cryptographic signature. A token is accepted without its signature being fully verified, which could allow an attacker to join an organization without a valid invitation.	6.8	More Details
CVE-2026-19129	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a network-positioned attacker to intercept backup data due to improper verification of the backup server's identity. The identity of the backup server is not verified when the secure connection for analytics backups is established, which could allow backup data, and credentials if used, to be intercepted.	6.8	More Details
CVE-2026-121796	The Add From Server Lite WordPress plugin before 6.0.0 does not restrict SVG uploads to users allowed to post unfiltered HTML, allowing users with the Author role and above to upload SVG files containing JavaScript and perform Stored XSS attacks.	6.8	More Details
CVE-2026-111771	The Model Context Protocol TypeScript SDK provides TypeScript client and server implementations of the Model Context Protocol. From 1.6.0 until 1.32.0 in @modelcontextprotocol/sdk, from 2.0.0 until 2.3.0 in @modelcontextprotocol/server, from 2.0.0 until 2.0.2 in @modelcontextprotocol/express, and from 2.0.0 until 2.3.1 in @modelcontextprotocol/server-legacy, server-side bearer authentication could accept a valid access token issued for a different service because the SDK did not enforce the token audience. The affected surface is server-side HTTP bearer authentication. The trigger is a valid token whose audience names another service. The authorization server must issue tokens for multiple services, and the application's verifyAccessToken() must not independently validate aud. Applications already validating aud inside verifyAccessToken() are not affected. An attacker with a token for another service could authenticate to the MCP server and obtain the confidentiality and integrity capabilities granted to an authenticated caller. Upgrading alone leaves the new audience validation disabled. Operators must enable audience validation and provide the token audience together. Enabling only the expected audience check causes every request to receive HTTP 401. This issue is fixed in @modelcontextprotocol/sdk 1.32.0, @modelcontextprotocol/server 2.3.0, @modelcontextprotocol/express 2.0.2,	6.8	More Details

	and @modelcontextprotocol/server-legacy 2.3.1.		
CVE-2026-119073	The Live Composer WordPress plugin before 2.1.23 does not escape a pagination setting supplied through its post-listing module shortcodes before outputting it in an HTML attribute, allowing users with the Contributor role and above to perform Stored Cross-Site Scripting attacks.	6.8	More Details
CVE-2026-109081	A flaw was found in Keycloak. The Dynamic Client Registration (DCR) endpoint does not properly validate authorization when processing the deprecated defaultRoles field. An authenticated attacker with client creation privileges or an Initial Access Token (IAT) can inject excessive roles into the realm's default roles configuration. This causes clients across the realm to generate bloated access tokens, resulting in performance and memory degradation that can lead to a Denial of Service (DoS).	6.8	More Details
CVE-2026-123618	ABP Framework before 10.7.1 contains an authentication bypass vulnerability that skips account state and two-factor checks when password login succeeds through a registered IExternalLoginProvider. Attackers holding the external directory password for deactivated, locked, or 2FA-protected accounts can obtain valid access tokens from the /connect/token password grant.	6.8	More Details
CVE-2026-17368	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to perform network reconnaissance and obtain sensitive credentials due to server-side request forgery. The server can be made to send requests to unintended destinations and return the results.	6.8	More Details
CVE-2026-123619	Lektor through 3.3.14 and 3.4.0b15 contains an absolute path traversal vulnerability in the admin API on Windows that allows attackers to escape the project directory by supplying drive-letter paths that cleanup_path does not normalise. Attackers can use a malicious web page with cross-site requests or DNS rebinding against the unauthenticated local server to recursively delete directories via deleterecord or write attacker-controlled files via newattachment.	6.8	More Details
CVE-2026-106649	The Kali Forms — Contact Form & Drag-and-Drop Builder WordPress plugin before 2.4.29 does not prevent users with author-level access and above from storing arbitrary JavaScript in a form button configuration, which is later output into a JavaScript execution context and runs in the browser session of any user who clicks the button, including an administrator.	6.8	More Details
CVE-2026-105259	The Easy Social Icons WordPress plugin before 4.0.3 does not sanitise SVG files, which it adds to the list of file types that may be uploaded site-wide, allowing users with the Author role and above to upload a malicious SVG containing XSS payloads. Where another installed Easy Social Icons WordPress plugin before 4.0.3 exposes an upload route to unauthenticated visitors, the same issue can be triggered without an account.	6.8	More Details
CVE-2026-19688	A flaw was found in the Admin REST API of Keycloak, an identity and access management solution. The Admin API fails to verify the intended audience of bearer tokens during authentication. This issue allows an attacker who operates a client within a realm to capture an administrator's access token and reuse it to perform unauthorized administrative actions, potentially leading to full realm compromise.	6.8	More Details
CVE-2026-17128	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to the insertion of sensitive information into log files.	6.8	More Details
CVE-2026-85347	The FV Flowplayer Video Player WordPress plugin before 7.5.56.7212 does not sanitize and escape a user-supplied value before outputting it in a page, which could allow users with the Contributor role and above to inject arbitrary web scripts that execute when a higher-privileged user views the affected page.	6.8	More Details
CVE-2026-118983	The VikWidgetsLoader WordPress plugin before 1.12.3 does not sanitise or escape several block attributes before outputting them inside HTML attributes, allowing users with the Contributor role to store arbitrary JavaScript that executes in the browser of any user viewing the affected post, including the administrator or editor who reviews the pending submission.	6.8	More Details
CVE-2026-107786	The CatFolders WordPress plugin before 2.5.7 does not properly sanitize and escape a user-controlled sort setting before using it in a SQL query, allowing authenticated users with upload capability (Author and above) to perform SQL injection attacks.	6.8	More Details
CVE-2026-123297	In JetBrains Hub before 2026.2.52519 two-factor authentication bypass was possible via the password reset flow	6.8	More Details
CVE-2026-123283	In JetBrains Datalore before 2026.4 account takeover was possible via SSO sign-in to a pre-registered account	6.8	More Details
CVE-2026-115250	The Text Typing WordPress plugin before 2.2.2 does not properly sanitize and escape a block attribute before storing it and later outputting it into a page element that is read and rendered by client-side script, allowing users with the Contributor role and above to perform Stored Cross-Site Scripting attacks that execute in the browser of anyone viewing the affected page.	6.8	More Details
CVE-2026-94395	A stack-based buffer overflow in Thales SafeNet Authentication Client (SAC) SIS token engine processing can be triggered by a malicious physical or software-emulated smart card. The issue can occur before authentication or PIN entry and may cause a denial of service or potentially arbitrary code execution with the privileges of the	6.8	More Details

	affected process. Affected releases start with SAC 10.8 R7 and include SAC 10.9 R3 GA (build 10.9.7449).		
CVE-2026-92396	The ShopEngine Gutenberg WooCommerce Builder Blocks Addon WordPress plugin before 2.4.4 does not validate the user's capabilities or the ownership of the targeted post in one of its AJAX actions, and does not escape the stored value before outputting it in a JavaScript context, allowing users with a role as low as contributor to inject arbitrary scripts into any post that will run when a higher privileged user edits it.	6.8	More Details
CVE-2026-118783	The All-in-One Video Gallery WordPress plugin before 5.0.0 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embedded, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	6.8	More Details
CVE-2026-123307	In JetBrains IntelliJ IDEA before 2026.3, 2026.2.4 unauthenticated connection to an arbitrary host via run configurations was possible	6.8	More Details
CVE-2026-97174	A flaw was found in the Client-Initiated Backchannel Authentication (CIBA) implementation of Keycloak. The CIBA endpoint fails to properly validate the sub parameter, allowing it to be stored as an additional request parameter. During the token issuance process, this injected value overwrites the legitimate subject identifier. This allows an attacker to authenticate as themselves but receive security tokens belonging to a different victim user, leading to unauthorized account access.	6.8	More Details
CVE-2026-118785	Improper handling of non-secure-world input in NSC veneer functions of NXP MCUXpresso SDK TrustZone-M examples (trustzone_examples), affecting versions through 26.06.00-lts and 26.09.00-pvw2, may allow a non-secure caller to supply unvalidated pointers or untrusted data, causing a timing side-channel, TOCTOU condition, or format-string misuse, potentially resulting in secure-world memory disclosure or denial of service. All software versions starting from 26.06.01-lts and 26.09.00 have fixed this issue.	6.7	More Details
CVE-2026-123037	A flaw was found in the ansible-core user module. When generate_ssh_key is enabled, User.ssh_key_gen() guards the key files against symlinks but checks the ~/.ssh directory only with os.path.exists(). An unprivileged user on a managed node who replaces their ~/.ssh with a symlink to an existing root-writable directory causes the privileged module to write the generated key pair through the symlink and then chown both files to that user. Because such files can be dropped into directories processed by schedulers (e.g. /etc/cron.daily) or dynamic MOTD (/etc/update-motd.d), the user can escalate to root on the managed node. This is an incomplete fix of CVE-2024-9902.	6.7	More Details
CVE-2026-123278	In JetBrains IntelliJ IDEA before 2026.3 code execution was possible via the unauthenticated JDBC worker RMI endpoint	6.7	More Details
CVE-2026-115452	Joomla Extension - tassos.gr - Privileged stored XSS in Advanced Custom Fields 2.8.2-2.8.15, 3.0.0-3.1.8 and Smile Pack 1.1.2-1.2.9, 2.0.0-2.1.6 - A user who could edit a Map marker label, like an article author, could add a script that ran for anyone who opened the marker.	6.7	More Details
CVE-2026-115243	The WPvivid — Backup, Migration & Staging WordPress plugin before 0.9.137 does not validate the extension of the file it actually stores when handling an import upload: it checks the extension of a separate request field while saving the uploaded file itself with WordPress's upload type-checking disabled, so an authenticated administrator can store a file with an arbitrary extension, including a PHP file, in the WPvivid — Backup, Migration & Staging WordPress plugin before 0.9.137's import directory. This is an incomplete fix of CVE-2025-5961, whose extension check was applied to the wrong value.	6.7	More Details
CVE-2026-122137	Powerlevel10k before 1.20.19 contains an insecure temporary directory vulnerability in the bundled gitstatus/install script that reuses attacker-creatable directories when mktemp fails. Local attackers can pre-create the predictable gitstatus-install.tmp directory to replace the extracted gitstatusd binary, which then executes with the victim's privileges.	6.7	More Details
CVE-2026-111253	A flaw was found in dnf5daemon-server. Session methods on dynamically exported D-Bus session objects do not verify that the caller is the unique sender that created the session. A local attacker can modify another user's live package-management session and replace its resolved transaction plan. If the legitimate session party later authorizes execution, the root daemon may apply the attacker-chosen package operations.	6.6	More Details
CVE-2026-76181	LibreOffice includes a dBASE database driver, which reads dBASE tables and their .ndx index files when a folder of dBASE files is used as a data source. A heap buffer overflow existed when an index page was read. The number of entries recorded in a page was not checked against the number of entries the page could hold, which comes from a different field of the index header. A crafted index could also make a page refer back to itself, so that reading it recursed without end. In fixed versions the index header and the entry count of each page are limited to what an index page can hold, and a page that refers back to one of its parent pages is not followed.	6.6	More Details
CVE-2026-121925	A stack-based buffer overflow in libsnowflakeclient and the Snowflake PHP PDO Driver could, under specific conditions, result in memory corruption during SAML-based authentication. During a native SSO/SAML login flow, the affected drivers may have copied a value taken from the identity provider's HTML response into a fixed-size memory buffer without first validating the length of that value. An attacker who controlled or had compromised the configured identity provider — or who was able to redirect the SAML single sign-on endpoint to an attacker-controlled server — might have leveraged this by returning an oversized response, potentially resulting in a crash or, in specific circumstances, remote code execution within the context of the application running the library. The fix is available in libsnowflakeclient version 2.11.1 and Snowflake PHP PDO Driver version 4.3.0. Users must	6.6	More Details

	manually upgrade.		
CVE-2026-95652	Execution with unnecessary privileges vulnerability in TÜBİTAK BİLGEM Software Technologies Research Institute pardus-usb-formatter allows Privilege Abuse. This issue affects pardus-usb-formatter: from 0.7.0 before 0.7.2.	6.6	More Details
CVE-2026-105422	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in TÜBİTAK BİLGEM Software Technologies Research Institute pardus-boot-repair allows Path Traversal. This issue affects pardus-boot-repair: from 1.0.9 before 1.1.0.	6.6	More Details
CVE-2026-12967	The WCFM Membership WordPress plugin before 2.12.1 does not verify that payment was made before completing a paid membership, allowing any authenticated Subscriber/Customer to activate a paid vendor membership for free and gain the marketplace vendor role.	6.5	More Details
CVE-2026-69145	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to 7.15.2 and 8.10.2, AOR report generation reloads the value stored in aor_fields.field and concatenates it into report SQL without strict field validation. An authenticated user able to configure reports can inject SQL through that stored field value and disclose database contents. This issue is fixed in versions 7.15.2 and 8.10.2.	6.5	More Details
CVE-2026-17307	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to broken object-level authorization.	6.5	More Details
CVE-2026-121954	FreeRDP before 3.32.2 has a heap out-of-bounds write in the planar codec because freerdp_bitmap_planar_context_reset commits new dimensions before buffer reallocation succeeds, and a failed ResetGraphics is only logged. A malicious RDP server can send an oversized ResetGraphics PDU, then a GFX PLANAR command, to corrupt client heap memory and crash the client.	6.5	More Details
CVE-2026-121783	Cross-Site Request Forgery (CSRF) vulnerability in Passionate Programmer Peter WP Data Access wp-data-access allows Cross Site Request Forgery.This issue affects WP Data Access: from n/a through 5.5.90.	6.5	More Details
CVE-2026-123856	In JetBrains Toolbox App before 3.6.1 nTLM hash disclosure was possible via SVG tool icons from a Remote Development server	6.5	More Details
CVE-2026-100359	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to 7.15.2 and 8.10.2, the Project Template module's action_get_end_date function interpolates authenticated caller-controlled task_id and lag POST parameters directly into SQL without sanitization, parameterization, or escaping. Any authenticated user can perform blind SQL injection to read customer data, internal communications, credentials, and other database contents. This issue is fixed in versions 7.15.2 and 8.10.2.	6.5	More Details
CVE-2026-19134	A vulnerability in OpenText OpenText Directory Services (OTDS) allows Black Box Reverse Engineering. This issue affects OpenText Directory Services (OTDS): from 22.1 to 26.2	6.5	More Details
CVE-2026-116572	FreeSWITCH is an open-source software telecommunications platform. From 1.10.0 to 1.11.1, there is a stack-based buffer overflow in mod_sofia when processing SIP Contact display names for dialog-event notifications. A peer can establish a dialog containing an excessively long display name and subsequently subscribe to that entity's dialog events, causing the stored value to overflow a fixed 512-byte stack buffer. Exploitation requires presence management to be enabled, directly or through shared appearance, and normally requires valid profile credentials unless subscription authentication is disabled. The overflow can terminate the FreeSWITCH process and all active calls. This vulnerability is fixed in version 1.11.2.	6.5	More Details
CVE-2026-123997	Hisense VIDAA Smart TV firmware V0000.01.00a.P0220 contains an unauthenticated denial-of-service vulnerability in the UPnP/DLNA AVTransport SOAP service that allows LAN-adjacent attackers to freeze the entire television software layer by sending a crafted SetAVTransportURI request on TCP port 38400. Attackers can exploit this flaw without credentials to render the device completely unresponsive to remote control or front-panel input, requiring a physical power cycle to restore functionality.	6.5	More Details
CVE-2026-116573	FreeSWITCH is an open-source software telecommunications platform. From 1.10.0 until 1.11.1, a stack-based buffer overflow in mod_sofia when generating dialog-event notifications. A peer can establish a dialog with an excessively long SIP To-header user part and subsequently subscribe to that entity's dialog events, causing the stored value to overflow a fixed-size stack buffer. Exploitation requires presence or shared-appearance management to be enabled and normally requires valid profile credentials, unless subscription authentication is disabled. The overflow can terminate the FreeSWITCH process and all active calls. This vulnerability is fixed in version 1.11.2.	6.5	More Details
CVE-2026-63663	CloudBeaver is a cloud database manager. From version 23.2.3 until 26.1.2, a path traversal vulnerability in its SQL result-editing functionality allows an authenticated user with SQL result-editing privileges to cause the server to open files outside the intended temporary upload directory. In affected database value-handling scenarios, this can disclose local files readable by the CloudBeaver server process. Version 26.1.2 prevents traversal outside the intended temporary upload directory.	6.5	More Details
CVE-	Joomla Extension - tassos.gr - File deletion through improper access control in Advanced Custom Fields extension		

2026-115451	2.8.13-2.8.15, 3.1.4-3.1.8 and Smile Pack 1.2.7-1.2.9, 2.1.2-2.1.6 - Anyone could delete images in the Gallery folders, including images on published articles and modules, without logging in. In ACF 3.1.7 and 3.1.8, users could also see, remove or save each other’s unsaved uploads.	6.5	More Details
CVE-2026-63664	CloudBeaver is a cloud database manager. In versions up to and including 26.1.1, some server-side export operations do not consistently enforce the global data export restriction. An authenticated non-administrative user with access to a shared database connection can initiate certain server-side data exports even when an administrator has disabled exports. This can disclose database contents that the user is permitted to query but is not permitted to export. The issue does not grant additional database read privileges. It is fixed in 26.1.2 by consistently enforcing the global restriction for server-side exports.	6.5	More Details
CVE-2026-103914	The Dynific Addons for Elementor plugin for WordPress is vulnerable to SQL Injection via the 'q' parameter in versions up to, and including, 1.3. This is due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query in the ae_preview_post() AJAX handler and its preview_post_filter() posts_where callback, where the value is passed through $wpdb->esc_like() (addcslashes for '_%\\') and concatenated into a single-quoted SQL LIKE literal — a construction that does not escape single quotes and actively escapes the backslash wp_magic_quotes places before the attacker's quote, freeing it to terminate the literal. This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	6.5	More Details
CVE-2026-122007	Oqtane Framework before 10.3.0 contains a broken access control vulnerability in SettingController.cs that allows an authenticated site administrator to read and modify settings belonging to other sites within the same tenant database by supplying an arbitrary entityId for Site or Role type settings, since IsAuthorized and FilterPrivate fail to verify the requested site matches the current alias SiteId. Attackers can exploit the /api/setting endpoints to disclose private values such as SMTPPassword, SMTPClientSecret, and ExternalLogin ClientSecret, and to alter another site's OIDC/OAuth2 authentication configuration without requiring host privileges.	6.5	More Details
CVE-2026-107359	Improper input validation in the beacon handler for WF200 firmware versions 3.17.0 and earlier may result in a divide-by-zero fault.	6.5	More Details
CVE-2026-114456	Multiple Snowflake client drivers implementing the `authenticator=externalbrowser` single sign-on flow could have allowed an attacker to interfere with a user's login attempt through weaknesses in the local loopback callback listener used to receive the identity provider's response. The listener reflected an arbitrary request's Origin header into its CORS response headers and accepted the first token-bearing request it received during the login window without verifying a CSRF state value bound to that specific login attempt. An attacker able to reach the listener during an active login might have leveraged this to submit a forged callback response, causing the authentication attempt to fail. The fix is available in Snowflake Connector for Python 4.8.0, Snowflake Go Driver v2.3.0, Snowflake JDBC Driver 4.4.0 (including the snowflake-jdbc-fips and snowflake-jdbc-thin artifacts), Snowflake Node.js Driver 3.4.0, Snowflake Connector for .NET 6.3.0, Snowflake ODBC Driver 4.0.0, Snowflake PHP PDO Driver 4.3.0, and libsnowflakeclient 2.11.1. Go v1 users must migrate to the latest major version of the module. Users must manually upgrade.	6.5	More Details
CVE-2026-62852	FreeScout is a self-hosted help desk and shared mailbox. Prior to 1.8.226, RealtimeConvNewThread checks only general mailbox access and does not apply the conversation-level restriction for users configured to see only assigned conversations. A restricted authenticated user can subscribe to predictable conv.<conversation_id> Polycast channels for other conversations in the same mailbox. New event payloads can expose complete replies, internal notes, recipient addresses, conversation state, assignee data, attachment names, and attachment URLs containing valid download tokens. This issue is fixed in version 1.8.226.	6.5	More Details
CVE-2026-104134	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to 8.3.0, the search_persons action in library/ajax/person_search_ajax.php validates CSRF but does not perform an AclMain authorization check before searching the person and patient_data tables. A low-privilege authenticated user can iterate name prefixes and receive patient first and last names, dates of birth, gender, phone numbers, and email addresses in JSON responses. This issue is fixed in version 8.3.0.	6.5	More Details
CVE-2026-17310	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote attacker to obtain sensitive information due to the use of a hard-coded cryptographic key.	6.5	More Details
CVE-2026-69144	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to 7.15.2 and 8.10.2, download.php checks authorization against a Documents bean before resolving whether the supplied identifier is a document_revisions.id. When a revision UUID is submitted with type=Documents, the check targets an empty Documents bean; the revision is then resolved and served without checking its parent document. A low-privileged authenticated user can use this identifier confusion to download administrator-owned or otherwise protected documents. This issue is fixed in versions 7.15.2 and 8.10.2.	6.5	More Details
CVE-2026-85287	HomeBox is a home inventory and organization system. Prior to 0.27.0, POST /api/v1/users/register and the users.email uniqueness constraint treat email addresses as case-sensitive while HomeBox uses a case-insensitive login lookup. An unauthenticated attacker who knows a victim's email can register a differently cased variant, creating duplicate rows that cause login to return 401 for both variants and deny the victim access, while also bypassing the one-account-per-email policy. This issue is fixed in version 0.27.0.	6.5	More Details

CVE-2026-121579	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 Stored XSS.This issue affects Unlimited Elements For Elementor (Free Widgets, Addons, Templates): from n/a through 2.0.26.	6.5	More Details
CVE-2026-121950	FreeRDP before 3.32.2 does not check the product of surface dimensions in gdi_CreateSurface when handling an RDPGFX CREATE_SURFACE PDU, causing an integer wrap and heap buffer overflow on 32-bit builds and an approximately 4 GiB allocation on 64-bit builds. A malicious RDP server can send a CREATE_SURFACE PDU with width and height 32766 to a connecting client to corrupt heap memory or cause a denial of service.	6.5	More Details
CVE-2026-120364	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Untapwp Vidplex vidplex allows Stored XSS.This issue affects Vidplex: from n/a through 1.0.3.	6.5	More Details
CVE-2026-104138	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to 8.3.0, custom/ajax_download.php, custom/download_qrda.php, custom/export_qrda_xml.php, and custom/qrda_download.php validate CSRF but do not enforce the patients/med ACL used by the canonical CQM report page. The endpoints also accept an unscoped report_id, allowing a low-privilege authenticated user to reach report generation and download logic for other reports. In a clinic with generated CQM reports, this can expose QRDA Category One and Category Three clinical documents for patients in a measure. This issue is fixed in version 8.3.0.	6.5	More Details
CVE-2025-71454	vtenext before 25.02.2 contains a cross-site request forgery protection bypass because csrf_check() in include/utils/VteCsrf.php skips __csrf_token validation for non-POST requests. Attackers can induce a logged-in user to open a crafted link sending state-changing GET requests, which handlers read from $_REQUEST, performing actions as that user.	6.5	More Details
CVE-2026-77463	Remark42 is a self-hosted comment engine for blogs, articles, or any other place where readers can add comments. From 1.0.0 until 1.16.2, Remark42 globally trusts True-Client-IP, X-Real-IP, and X-Forwarded-For without verifying that the direct peer is a trusted proxy, and middleware.RealIP overwrites r.RemoteAddr before per-IP controls run. In a directly reachable deployment, or a proxy that forwards attacker-controlled headers, a remote attacker can rotate spoofed forwarding headers to obtain fresh token buckets for rate-limited endpoints, bypass vote de-duplication when --votes-ip is enabled, mint anonymous identities, and poison stored comment IPs and request logs. The global concurrent-request throttle and per-request timeouts still limit availability impact. Mitigation support is available in version 1.16.2, but operators must configure --trusted-proxy for the deployment topology.	6.5	More Details
CVE-2026-97701	Zulip is an open-source team collaboration tool. In Zulip Server versions through 12.1, the authenticated POST /messages/render endpoint renders the content parameter without enforcing the normal message length limit used by message send and edit operations. An authenticated user can submit Markdown up to the server body-size limit, causing disproportionate backend CPU consumption, and repeated or concurrent requests can degrade Markdown rendering performance or backend availability for other users. This issue is fixed in version 12.2.	6.5	More Details
CVE-2026-122669	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Everest Forms Everest Forms everest-forms allows Stored XSS.This issue affects Everest Forms: from n/a through 3.6.3.	6.5	More Details
CVE-2026-121784	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Magepeople inc. WpBookingly service-booking-manager allows Stored XSS.This issue affects WpBookingly: from n/a through 1.4.3.	6.5	More Details
CVE-2026-123125	The Symfony Validator component IpValidator incompletely classifies internal addresses in the filtered modes of the Ip constraint, so some internal addresses are accepted as public, which can lead to Server-Side Request Forgery (SSRF) in Symfony versions prior to 5.4.56, 6.x prior to 6.4.50, 7.x prior to 7.4.23, and 8.x prior to 8.1.11. In these modes, IpValidator relies on the PHP flags FILTER_FLAG_NO_PRIV_RANGE and FILTER_FLAG_NO_RES_RANGE to classify addresses as public, private, or reserved. These flags do not cover shared address space (100.64.0.0/10) or IPv4-mapped, IPv4-compatible, and 6to4 IPv6 addresses, which can embed internal IPv4 addresses. A value such as ::ffff:127.0.0.1 can therefore pass validation even though it points to an internal host. Applications that rely on the Ip constraint to reject internal addresses, for example before making a server-side request to a user-supplied address, can be exposed to SSRF.	6.5	More Details
CVE-2026-82029	Invoice Ninja before 5.13.28 contains a broken access control vulnerability that allows authenticated vendor-portal contacts to access documents belonging to other vendors and clients by exploiting authorization checks that validate only company_id scope instead of vendor ownership. Attackers can request GET /vendor/documents/{hashid}/download or POST /vendor/documents/download_multiple, enumerating predictable sequential Hashids document identifiers due to a default empty HASH_SALT, to read any invoice PDFs, contracts, payment receipts, and expense attachments within the company.	6.5	More Details
CVE-2026-123096	anacrolix/torrent through 1.61.0 contains a memory exhaustion vulnerability in the tracker/http package that allows malicious trackers to crash clients by returning unbounded responses. Attackers controlling an HTTP tracker in a torrent file or magnet link can return huge or gzip-compressed announce or scrape responses that Client.Announce and Client.Scrape buffer without limits, exhausting process memory.	6.5	More Details
	OpenEMR is a free and open source electronic health records and medical practice management application. Prior		

CVE-2026-104136	to 8.3.0, the new_recall branch of interface/main/messages/save.php accepts a caller-supplied pid without enforcing patient-level or recall-workflow authorization. A low-privilege authenticated user who knows or enumerates a patient identifier can retrieve patient details, contact fields, HIPAA notification preferences, recent appointment information, and existing recall information. This issue is fixed in version 8.3.0.	6.5	More Details
CVE-2026-102943	Dagu is a workflow engine with a built-in Web user interface. Prior to version 2.11.0, its MCP dagu_read operation with target dag_spec invokes the DAG specification API directly, bypassing the HTTP middleware introduced for CVE-2026-33344. The underlying resolver does not restrict resolved paths to configured DAG directories. An authenticated attacker with a viewer-role API key can supply an absolute or traversing path to read .yaml or .yml files outside those directories that are accessible to the Dagu process. The affected operation does not provide write or execution capability. This issue is fixed in version 2.11.0.	6.5	More Details
CVE-2026-119758	ERPNext OCR app for Frappe/ERPNext through 1.1.1 contains a missing authorization and path traversal vulnerability that allows any authenticated user to read arbitrary server files by passing a fully client-controlled path argument to the whitelisted read_document method. Attackers can supply local file paths to bypass Frappe's File doctype permission model and access other users' private uploads, or supply arbitrary URLs to trigger server-side requests reaching internal services and cloud metadata endpoints.	6.5	More Details
CVE-2026-88985	Kubeflow Pipelines enables users to build and deploy portable, scalable machine learning workflows. Prior to 2.17.0, the API server trusts structural SQL identifier fields decoded from the base64-encoded JSON page_token parameter before constructing list queries. An attacker who can invoke an affected pipeline or run list API can inject through KeyFieldName or SortByFieldName, including v1beta1 and v2beta1 run-listing metric paths, and read data available to the API server database account across namespaces. Database modification is not established. This issue is fixed in version 2.17.0.	6.5	More Details
CVE-2026-16719	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote attacker to view arbitrary files on the system due to a path traversal vulnerability. A specially crafted URL request could allow directories outside the intended location to be accessed.	6.5	More Details
CVE-2026-115739	Hard-coded Cryptographic Key vulnerability exists in the DLP on-prem extensions version 11.13.1 and earlier allows a remote attacker to decrypt credentials and evidence files.	6.5	More Details
CVE-2026-120365	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Aguila Technologies WP Customer Area customer-area allows Stored XSS.This issue affects WP Customer Area: from n/a through 8.4.3.	6.5	More Details
CVE-2026-121936	easyVoice before 0.0.23 contains a server-side request forgery vulnerability that allows unauthenticated attackers to make the server send POST requests by supplying openaiBaseUrl with useLLM enabled. Attackers can target loopback and internal services through /api/v1/tts endpoints, using reflected error messages in the x-generate-tts-warning header to probe internal hosts and ports.	6.5	More Details
CVE-2026-123273	ImageMagick before 7.1.2-35 and 6.9.13-60 contains an infinite loop vulnerability in the SVG decoder because QueueAuthenticPixelCacheNexus in MagickCore/cache.c fails to validate requested region width and height. Attackers can supply a crafted SVG image that repeatedly requests a non-advancing pixel region, consuming CPU and hanging the decoding worker.	6.5	More Details
CVE-2026-115241	The WPvivid — Backup, Migration & Staging WordPress plugin before 0.9.137 does not verify that a submitted snapshot identifier names a snapshot it actually created before using it as a database table-name prefix, so an authenticated administrator can supply the site's table prefix, or any other string, and cause the WPvivid — Backup, Migration & Staging WordPress plugin before 0.9.137 to drop every matching table, including the core WordPress tables, destroying the site's database.	6.5	More Details
CVE-2026-119501	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BdThemes Element Pack Elementor Addons bdthemes-element-pack-lite allows Stored XSS.This issue affects Element Pack Elementor Addons: from n/a through 10.0.2.	6.5	More Details
CVE-2026-119748	The GetPaid plugin for WordPress before 2.8.63 contains an authorization bypass vulnerability that allows unauthenticated attackers to access and manipulate another user's invoice by supplying its ID through the maybe_use_invoice parameter in process_invoice(), bypassing the ownership and key checks performed by is_authorized_to_pay(). Attackers can submit a known pending invoice ID via maybe_use_invoice to read checkout pricing details and initiate a checkout workflow, resulting in an unauthorized state change of the invoice to on-hold.	6.5	More Details
CVE-2026-120560	The Active Woot Products Tables for WooCommerce. 100% FREE plugin for WordPress is vulnerable to Media Library File Deletion in all versions up to, and including, 2.1.5 This is due to the `get_table_data()` AJAX handler — registered for unauthenticated access via `wp_ajax_nopriv_woot_get_table_data` — performing no nonce verification and no capability check before passing the attacker-supplied `wp_columns_actions` parameter directly to `apply_filters()` alongside an attacker-controlled integer derived from the `table_id` parameter. This makes it possible for unauthenticated attackers to delete any WordPress media library attachment and its underlying file in the uploads directory by supplying a known or guessed numeric attachment ID, enabling complete erasure of a site's media library. Exploitation is achievable because WordPress core registers `wp_delete_attachment()` as a callback on hooks such as `upgrader_scheduled_cleanup` and `importer_scheduled_cleanup`, which `sanitize_key()` does not strip; notably, only attachment posts reachable by	6.5	More Details

	numeric ID are affected, and files outside `wp-content/uploads` — such as `wp-config.php` or plugin PHP files — cannot be targeted through this path.		
CVE-2026-108262	DDEV is an open-source tool for running local web development environments for PHP and Node.js. From 1.25.2 until 1.25.4, Untar in pkg/archive/archive.go validates an absolute tar symlink target after rebasing it beneath dest, but creates the symlink with the raw absolute Linkname. A crafted archive can therefore plant a host-absolute symlink and use a following regular-file entry to write outside the extraction directory. The flaw is reachable through remote add-on retrieval and database or file imports, and overwriting shell startup files, Git hooks, or cron entries can lead to code execution in the DDEV user's context. Unzip is not affected. This issue is fixed in version 1.25.4.	6.5	More Details
CVE-2026-110964	The Essential Real Estate WordPress plugin before 5.3.5 does not verify that a media attachment belongs to the requesting user before deleting it, allowing a self-registered customer-level user to delete other users' media library attachments, including those owned by administrators.	6.5	More Details
CVE-2026-104139	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to 8.3.0, library/ajax/set_pt.php allows any authenticated user to set an arbitrary patient identifier in the active session without an ACL check, and interface/patient_file/download_template.php trusts that session value while enforcing only CSRF validation. A low-privilege user can select another patient and download a rendered document template containing the patient's demographics, encounter information, allergies, medications, and problem list despite lacking patients/docs access. This issue is fixed in version 8.3.0.	6.5	More Details
CVE-2026-121959	FreeRDP before 3.32.2 contains an infinite loop vulnerability in websocket_context_read that fails to handle a zero BIO result with payload outstanding. A malicious RD Gateway can send a truncated WebSocket frame followed by a TLS close_notify, causing a client thread to spin and consume CPU until killed.	6.5	More Details
CVE-2026-118639	The Surfer WordPress plugin before 1.8.1.759 discloses a sensitive API credential to low-privileged users through the post editor page and relies on that same credential as the sole authorization for its privileged REST API, allowing users with contributor-level access and above to read the credential and escalate to publishing arbitrary posts and other privileged actions.	6.5	More Details
CVE-2026-111769	The Model Context Protocol TypeScript SDK provides TypeScript client and server implementations of the Model Context Protocol. Prior to 1.32.0 in @modelcontextprotocol/sdk and from 2.0.0 until 2.3.0 in @modelcontextprotocol/client, the HTTP client transports and OAuth client requests followed redirects to a different origin while retaining custom request headers and, for HTTP 307 or 308 responses, request bodies. The affected surfaces are StreamableHTTPClientTransport, SSEClientTransport, and OAuth client functions such as auth(). The trigger is an HTTP redirect to another origin. Custom headers and mcp-session-id can be re-sent to the redirected origin. HTTP 307 and 308 redirects can also re-send the request body. OAuth request bodies can contain refresh_token and client_secret values. Current runtimes already strip the Authorization header across origins. stdio clients do not use the affected HTTP path. A malicious or compromised MCP or authorization server could therefore receive API keys, session identifiers, OAuth refresh tokens, or OAuth client secrets. Restoring unrestricted redirect following after upgrading restores the exposure. This issue is fixed in @modelcontextprotocol/sdk 1.32.0 and @modelcontextprotocol/client 2.3.0.	6.5	More Details
CVE-2026-123205	accel-ppp before 1.15.0 contains a heap buffer overflow vulnerability in the tcp, syslog and pgsql log targets that allows unauthenticated remote peers to overflow fixed heap buffers by producing log lines exceeding LOG_MAX_SIZE. Attackers within client-ip-range can send an L2TP Start-Control-Connection-Request with many string AVPs when verbose logging is enabled to corrupt heap memory and crash the daemon.	6.5	More Details
CVE-2026-63218	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to 7.15.2 and 8.10.2, the changeReportPage controller action renders a protected report without repeating the record-level access check enforced by DetailView. The affected flow begins at AOR_Reports and uses changeReportPage, and DetailView to carry attacker-controlled data or authorization state into the security-sensitive operation. An authenticated user can directly invoke the action and read report rows and restricted-module data despite owner-only or role-based report visibility. This issue is fixed in versions 7.15.2 and 8.10.2.	6.5	More Details
CVE-2026-115474	Zulip is an open-source team collaboration tool. From 8.0 until 12.2, in organizations where the Who can view all other users in the organization setting restricted guests from viewing other users, saving or editing a direct message draft did not verify that the sender could access the draft recipients. A guest could thereby gain access to otherwise restricted users' profile information without sending a message. Organizations that did not restrict guest access were unaffected. This issue is fixed in version 12.2.	6.5	More Details
CVE-2026-123477	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Crocoblock JetEngine jet-engine allows Stored XSS.This issue affects JetEngine: from n/a through 3.9.0.2.	6.5	More Details
CVE-2026-122032	SPIP before 4.4.29 contains a SQL injection vulnerability that allows authenticated attackers with back-office access to inject arbitrary SQL by submitting a differing where parameter value in the POST body versus the GET query string on the /ecrire/?exec=articles endpoint, bypassing spip_sanitize_from_request() sanitization. Attackers can exploit this request parameter mismatch to extract database contents, including protected articles and bcrypt password hashes of users.	6.5	More Details
CVE-	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to 8.3.0, the sms_search branch of interface/main/messages/save.php requires an authenticated session but does		More

2026-104137	not enforce patient or feature-level ACLs. A low-privilege user who cannot access patient data through the normal interface can search the MedEx SMS endpoint and receive patient identifiers, names, phone numbers, SMS permission status, and recent message information. This issue is fixed in version 8.3.0.	6.5	Details
CVE-2026-63217	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to 7.15.2 and 8.10.2, the generatePdf entry point loads an arbitrary record through BeanFactory::getBean() without checking the requesting user's record access. The affected flow begins at modules/AOS_PDF_Templates/generatePdf.php and uses generatePdf, and BeanFactory::getBean() to carry attacker-controlled data or authorization state into the security-sensitive operation. Any authenticated user can read fields from records denied by configured ACL roles, including contact, financial, deal, and custom-field data. This issue is fixed in versions 7.15.2 and 8.10.2.	6.5	More Details
CVE-2026-17241	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to improper authorization.	6.5	More Details
CVE-2026-102564	The The Dynific Addons for Elementor (formerly Anywhere Elementor) plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 1.3.0 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. Exploitation requires the target site to have a public post rendered through an AE template that includes the AE Post Comments widget, and for the attacker's comment to be visible on that page — a barrier removed once the attacker has a previously approved comment or when comment moderation is relaxed.	6.5	More Details
CVE-2026-17240	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote attacker to bypass security restrictions due to improper authentication. Authentication checks are not applied consistently, which could allow protected resources to be reached without valid credentials.	6.5	More Details
CVE-2026-104135	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to 8.3.0, library/ajax/payment_ajax.php validates a CSRF token but performs no AclMain authorization check before executing a wildcard search of patient_data. Any authenticated user, including a non-clinical role, can enumerate patient identifiers, full names, and dates of birth through the set_patient branch. This issue is fixed in version 8.3.0.	6.5	More Details
CVE-2026-121620	CoopCycle coopcycle-web 5.6.0 before 6.20.0 contains a missing authentication vulnerability that allows unauthenticated attackers to forge Zelty webhook events because the x-zelty-hmac-sha256 HMAC signature is never verified. Attackers can POST forged dish, menu, option and order-status events to /api/zelty/webhook/* endpoints to toggle restaurant products and alter order preparation states.	6.5	More Details
CVE-2026-112336	Wazuh Manager from 3.0.0 before 4.14.9 contains a memory leak vulnerability in the generic JSON decoder that allows remote attackers to exhaust wazuh-analysisd memory via repeated static fields. Attackers can enroll an agent through passwordless enrollment and send events with duplicate fields such as id, triggering an OOM kill that disables alerting.	6.5	More Details
CVE-2026-81734	Missing Authorization in ProductEvents in Apache OFBiz 24.09 before 24.09.08 on all platforms allows a remote authenticated attacker holding only catalog view permission to create, modify, or remove arbitrary product, product feature association, and product category association data by directly invoking catalog quick-admin events such as updateProductQuickAdminShipping, causing the servlet to authorize the request against the base view-level permission declared on the request-map while the underlying event methods perform entity-engine writes without checking the catalog update/create permission enforced by equivalent sibling event methods in the same class. Users are recommended to upgrade to version 24.09.08, which fixes this issue.	6.5	More Details
CVE-2026-100228	Improper Input Validation in Order Returns in Apache OFBiz 24.09.07 on all platforms allows an authenticated user without the ORDERMGR_CREATE permission to persist an arbitrary price on a return item via the createReturnItem service, bypassing the intended server-computed price ceiling. Users are recommended to upgrade to version 24.09.08, which fixes this issue.	6.5	More Details
CVE-2026-97355	Use of Hard-coded Password vulnerability in the AdminServer component in Apache OFBiz 24.09.07 on all platforms allows an attacker able to reach the AdminServer control port to query the server's running state and trigger an unauthenticated shutdown of the instance via the fixed default control key shipped in start.properties. Users are recommended to upgrade to version 24.09.08, which fixes this issue.	6.5	More Details
CVE-2026-12067	Missing exception handlers in AvastSvc native message dispatcher (ashServ.dll) on Windows allow a local, unprivileged attacker to crash the service by sending specially crafted JSON messages. The vulnerability spans multiple handler pathways in the RPC-based native message protocol: * Log_NmSvc.message handler: converts JSON fields to strings without type validation and without exception boundaries. * OpenInSz_NmSvc handler: converts URL and origin fields to strings without type checking, exposing an exception. * OpenInSz_NmSvc.profile handler: converts the profile field to an integer without validation. In all three cases, the exceptions are not caught by action-specific handlers and propagate up the dispatcher. The common root cause is the absence of try-catch blocks around JSON type conversions in the native message processing chain.	6.5	More Details
CVE-2026-	Authentication bypass by Assumed-Immutable data vulnerability in Apache OFBiz. Apache OFBiz's optional Janrain Engage Social Login integration in the ecommerce component improperly binds authenticated external identities to local user accounts. This issue affects Apache OFBiz: before 24.09.08. Users are recommended to upgrade to	6.5	More Details

114277	version 24.09.08, which fixes the issue.		
CVE-2026-114272	Authorization Bypass Through User-Controlled Key in the content viewing component in Apache OFBiz 24.09 before 24.09.08 on all platforms allows an authenticated user with role-scoped content view permission to read the data of content they are not authorized to view via a ViewSimpleContent request that combines a contentId they can view with the dataResourceId of other content. Users are recommended to upgrade to version 24.09.08, which fixes this issue.	6.5	More Details
CVE-2026-114271	Authorization Bypass Through User-Controlled Key in the shopping list services in Apache OFBiz 24.09 before 24.09.08 on all platforms allows an authenticated low-privileged user, such as a self-registered ecommerce customer, to modify another party's shopping list or take ownership of it, and thereby read its contents, via a request to the shopping list update endpoint that supplies the other party's shopping list ID. Users are recommended to upgrade to version 24.09.08, which fixes this issue.	6.5	More Details
CVE-2026-114235	Direct Request ('Forced Browsing') in the Order component in Apache OFBiz 24.09 before 24.09.08 on all platforms allows an authenticated user with only view access to the Order Manager to modify the shipment tracking number of any order via a direct request to the updateTrackingNumber endpoint. Users are recommended to upgrade to version 24.09.08, which fixes this issue.	6.5	More Details
CVE-2026-109856	Direct Request ('Forced Browsing') to Financial Account services in Apache OFBiz 24.09 before 24.09.08 on all platforms allows an authenticated user with any valid low-privilege account to create, modify, and cancel financial account transactions and balances without appropriate permission via direct requests to the createFinAccount, updateFinAccount, deleteFinAccount, createFinAccountTrans, createFinAccountRole, createFinAccountAuth, setFinAccountTransStatus, and depositWithdrawPayments services. Users are recommended to upgrade to version 24.09.08, which fixes this issue.	6.5	More Details
CVE-2026-54377	VitaFit cloud API before 2026-10-30 contained an insecure direct object reference vulnerability that allows authenticated attackers to access another user's data by supplying a different user_id or profile_id to endpoints such as GET /front/profile/{profile_id}/report/ and GET /front/profile/{profile_id}/body_index_per_day/. Attackers can leverage predictable user_id and profile_id relationships combined with an account-enumeration weakness to read another account's email address, profile, body-composition report, and measurement history at scale.	6.5	More Details
CVE-2026-121794	The Travelly – Tour & Travel Booking Manager for WooCommerce plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 2.3.11 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 view stored WooCommerce payment gateway credentials — including PayPal API username, password, and signature, as well as Stripe test and live secret keys — injected verbatim into the HTML response of the tour edit screen. The credentials are present in the raw HTTP response regardless of the modal's CSS visibility state, making them trivially accessible by viewing page source.	6.5	More Details
CVE-2026-108949	Denial of Service via OOM vulnerability in Apache ActiveMQ, ActiveMQ Broker. An authenticated OpenWire client that sends a ConsumerInfo for a temporary queue/topic owned by another connection is rejected with InvalidDestinationException, but the rejected Subscription is left behind in the region's subscriptions map. Repeating the request leaks broker heap until OOM because the broker does not clean up the rejected subscriptions in the map. This issue affects Apache ActiveMQ: from 6.0.0 before 6.3.3, before 5.19.12; ActiveMQ Broker: from 6.0.0 before 6.3.3, before 5.19.12. Users are recommended to upgrade to version 6.4.0, 6.3.3, or 5.19.12, which fixes the issue.	6.5	More Details
CVE-2026-100168	Direct Request ('Forced Browsing') in the Content Manager component in Apache OFBiz 24.09.07 on all platforms allows an authenticated user holding only view-only content permissions (OFBTOOLS_VIEW and CONTENTMGR_VIEW) to re-parent content associations they do not own or manage via a direct POST request to the moveContentJson endpoint, which performs no permission check, unlike the equivalent updateContent/createContentAssoc/removeContentAssoc services that require genericContentPermission UPDATE. Users are recommended to upgrade to version 24.09.08, which fixes this issue.	6.5	More Details
CVE-2026-104992	The Booking for Appointments and Events Calendar – Amelia plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 9.9.1. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with custom-level access and above, to export a full CSV of booking records for any event on the site — including attendee names, email addresses, phone numbers, booking status, number of persons, price, payment status, payment amount, and coupon codes — regardless of whether they own or participate in those events.	6.5	More Details
CVE-2026-57562	Readest is a modern, feature-rich ebook reader designed for seamless cross-platform access and an intuitive reading experience. Prior to 0.11.10, POST /api/stripe/check in apps/readest-app/src/app/api/stripe/check/route.ts accepted a client-controlled sessionId, retrieved the corresponding Stripe Checkout Session, and granted the paid plan to the authenticated caller without verifying session.metadata.userId. The createOrUpdateSubscription path then updated the plans row keyed by the caller's user identifier rather than the Checkout Session owner. Any authenticated free user with a paid active Checkout Session identifier, including one from the user's own single legitimate purchase, could replay that identifier to upgrade additional accounts without payment. This issue is fixed in version 0.11.10.	6.5	More Details
CVE-2026-	The Directorist: AI-Powered Business Directory, Listings & Classified Ads WordPress plugin before 8.11 does not verify ownership of attachment IDs supplied when updating a listing's images, allowing authenticated users with	6.5	More

118532	Subscriber-level access and above to permanently delete arbitrary media library attachments, including those uploaded by administrators, along with their files.		Details
CVE-2026-57565	Readest is a modern, feature-rich ebook reader designed for seamless cross-platform access and an intuitive reading experience. Prior to 0.11.10, the apps/readest-app/src/pages/api/storage/upload.ts route constructed an object key from the authenticated user's identifier and a client-controlled fileName without rejecting path separators or parent-directory traversal. In the R2 backend, apps/readest-app/src/utils/r2.ts placed that key into a new Request URL before signing it, and URL normalization collapsed parent-directory components so the resulting presigned PUT could escape the caller's namespace. An authenticated attacker who knew a target user identifier and book hash could overwrite or poison that user's stored book object and corrupt the associated file_key metadata; the exact cross-tenant escape was verified for the R2 backend. This issue is fixed in version 0.11.10.	6.5	More Details
CVE-2026-108946	Improper input validation vulnerability in Apache ActiveMQ, Apache ActiveMQ KahaDB. The ActiveMQ broker resolves connection, session and consumer state from ids that are user provided and in some scenarios does not validate that they ids are bound to that user. This allows an authenticated client to spoof another user's ids. This allows: * an authenticated client consumes from another connection's temporary queue/topic by putting the victim's connection id in its own ConsumerId, bypassing the broker-side ownership check. * a duplicate ConsumerId registration is only logged, after which the attacker's RemoveInfo or disconnect tears down the victim's live subscription * a forged MessageAck for the victim's ConsumerId permanently deletes an in-flight, unacknowledged message. This issue affects Apache ActiveMQ: from 6.0.0 before 6.3.3, before 5.19.12; Apache ActiveMQ KahaDB: from 6.0.0 before 6.3.3, before 5.19.12. Users are recommended to upgrade to version 6.4.0, 6.3.3, or 5.19.12, which fixes the issue.	6.5	More Details
CVE-2026-110004	The wpForo Forum plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the theme_delete function in all versions up to, and including, 3.2.2 This makes it possible for authenticated attackers, with subscriber-level access and above, to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php). This exploit chain is reachable only on sites where an administrator has created a custom wpForo secondary usergroup with a blank WordPress role and the 'mth' (Manage Themes) capability; on such sites, an attacker can self-register and claim that group via the unguarded wpforo_secondary_groupids[] POST field, bypassing the role-based group filter and gaining theme-management access as a Subscriber.	6.5	More Details
CVE-2026-119489	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bootstrapped Ventures WP Recipe Maker wp-recipe-maker allows Stored XSS.This issue affects WP Recipe Maker: from n/a through 10.9.1.	6.5	More Details
CVE-2026-97356	External Control of File Name or Path vulnerability in the ViewFile component of Label Manager in Apache OFBiz 24.09.07 on all platforms allows an authenticated user holding only the LABEL_MANAGER_VIEW permission to read arbitrary properties and xml files on the server, including the generated JWT signing key, enabling forgery of an authenticated administrator session, via the fileName parameter of a ViewFile request. Users are recommended to upgrade to version 24.09.08, which fixes this issue.	6.5	More Details
CVE-2026-66981	HCL AION is affected by a vulnerability where the application trusted the value of the HTTP Host header supplied in requests without validation. An attacker could manipulate this header to influence links, redirects or responses generated by the application, potentially resulting in unintended behavior or security impact under certain conditions.	6.5	More Details
CVE-2026-119493	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Metaphor Creations, LLC Ditty ditty-news-ticker allows Stored XSS.This issue affects Ditty: from n/a through 3.1.71.	6.5	More Details
CVE-2026-81744	Incorrect Authorization in ContentPermissionServices in Apache OFBiz 24.09 before 24.09.08 on all platforms allows a remote authenticated attacker holding only a limited content-create permission to self-grant the OWNER role on arbitrary content by invoking the createContentRole service (e.g. via the createForumGroupRole request), causing the permission check to fall through to a fail-open default-grant branch when no ContentPurposeOperation entry matches the requested operation and content purpose, rather than denying the request. A self-granted OWNER role then satisfies the ownership check used to authorize update, removal, and status changes on that content, giving the attacker full read/write/delete control over content they should not have access to. Users are recommended to upgrade to version 24.09.08, which fixes this issue.	6.5	More Details
CVE-2026-103984	FreeScout is a self-hosted help desk and shared mailbox. Prior to 1.8.231, when limit_user_customer_visibility is enabled, the load_customer_info AJAX action performs a global lookup using an attacker-controlled customer email and checks only whether the agent can access a separately supplied mailbox. A non-admin agent can name an accessible mailbox and retrieve an unrelated customer's rendered profile without invoking CustomerPolicy::view(). The response can expose names, email addresses, phone numbers, company and job information, postal addresses, social profiles, websites, and confidential internal agent notes. This issue is fixed in version 1.8.231.	6.5	More Details
CVE-2026-120848	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WC Lovers WCFM Marketplace wc-multivendor-marketplace allows Stored XSS.This issue affects WCFM Marketplace: from n/a through 3.8.3.	6.5	More Details
CVE-	undici is an HTTP client for Node.js. In versions 7.0.0 through 7.30.1 and 8.0.0 through 8.12.3, when the redirect interceptor and a shared response cache are used together, an authenticated request that is redirected to a		

2026-120474	same-origin target has the final response stored under the original request's cache key. That key omits the credential and carries no Vary header, so a later anonymous or different user can be served the first user's private response body. This results in cross-user disclosure of cached private responses. The issue is fixed in undici 7.30.2 and 8.12.4, and users should upgrade to one of those versions or later.	6.5	More Details
CVE-2026-121768	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Markus Wiesenhofer Contact Form 7 – Post Fields cf7-post-fields allows Stored XSS.This issue affects Contact Form 7 – Post Fields: from n/a through 2.6.0.	6.5	More Details
CVE-2026-123284	In JetBrains Datalore before 2026.4 improper authorisation on workspace moves allowed view-only collaborators to modify shared content	6.5	More Details
CVE-2026-121792	The GamiPress – Gamification plugin to reward points, badges & ranks in WordPress, now with AI plugin for WordPress is vulnerable to generic SQL Injection via the 'input_<field_id>.<part> (Gravity Forms name-field part, or list-field row)' parameter in all versions up to, and including, 8.1.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. Exploitation requires a GamiPress achievement already configured against a Gravity Forms 'field value submission' event with the corresponding form published — a standard setup for sites using the integration.	6.5	More Details
CVE-2026-16725	IBM Watson Speech Services Cartridge 4.0.0 through 5.4.0 could allow a remote authenticated attacker to read arbitrary files from the local filesystem due to path traversal.	6.5	More Details
CVE-2026-81808	Missing Authorization in ProductSearchEvents in Apache OFBiz 24.09 before 24.09.08 on all platforms allows a remote authenticated attacker holding only catalog view permission to bulk-modify product category and feature associations across arbitrary search results by seeding a broad product search and then invoking search-result mutation events such as searchRemoveFromCategory, searchExpireFromCategory, searchAddToCategory, searchAddFeature, and searchRemoveFeature, causing the servlet to authorize the request against only the base view-level permission declared on the request-map while the underlying event methods perform bulk entity-engine deletes/inserts without checking the DELETE/CREATE permission enforced by the equivalent service-layer operations (e.g. removeProductFromCategory). Users are recommended to upgrade to version 24.09.08, which fixes this issue.	6.5	More Details
CVE-2026-110282	IBM Db2 Genius Hub 1.1.2, 1.1.3, 1.1.4, 1.1.5 could allow a remote authenticated attacker to bypass security restrictions due to improper access control.	6.5	More Details
CVE-2026-109994	The Eventin – Events Calendar, Tickets, Registration, Booking & WooCommerce plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 4.1.29 via the 'id' parameter. This makes it possible for authenticated attackers, with subscriber-level access and above, to extract the email address and phone number of any WordPress user, including administrators, by supplying their user id in a query-string parameter while placing the authenticated user's own id in the URL path.	6.5	More Details
CVE-2026-76152	Path traversal and missing authorization check in the imageCrop and imageRotate services in Apache OFBiz through 24.09.07 on all platforms allows a remote authenticated attacker with only Catalog view permission to read arbitrary image-parseable files readable by the OFBiz process, disclosed via re-encoded and republished product content, and to write a re-encoded image to an arbitrary directory writable by the OFBiz process via crafted productId and imageName parameters. Users are recommended to upgrade to version 24.09.08, which fixes this issue.	6.5	More Details
CVE-2026-76150	Path traversal and missing authorization check in the replaceImageToExistImage service in Apache OFBiz through 24.09.07 on all platforms allows a remote authenticated attacker with only Catalog view permission to overwrite arbitrary files writable by the OFBiz process with JPEG-encoded content via crafted productId, dataResourceNameExist, and dataResourceNameReplace parameters. Users are recommended to upgrade to version 24.09.08, which fixes this issue.	6.5	More Details
CVE-2026-66903	Authenticated Path Traversal in Catalog Image Management allows writing image files outside the intended directory in Apache OFBiz. This issue affects Apache OFBiz: before 24.09.08. Users are recommended to upgrade to version 24.09.08, which fixes the issue.	6.5	More Details
CVE-2026-115738	SQL injection vulnerability in DLP on-prem extensions version 11.13.1 and earlier allows a remote authenticated attacker to inject SQL queries without sanitization or parameterized queries.	6.5	More Details
CVE-2026-106716	ReelShort for Android version 3.8.55 loads an attacker-controlled activityUrl supplied through its cmsvictor://open deep link in a WebView that exposes the Android and Offerwall JavaScript bridges without validating the page origin. After a user opens the crafted link, the page can invoke getUserInfo, getCredentials, and initUser to obtain user metadata and an encrypted credential payload.	6.5	More Details
CVE-	Mongoose is an embedded web server and network library. Prior to 7.22, mg_path_is_sane in src/util.c read path.buf[1] without first requiring path.len to be at least two and read s[2] when only two bytes remained. Unauthenticated remote requests reaching mg_http_upload or mg_http_serve_dir with the affected short path		More

2026-115473	shapes could therefore trigger one-byte heap out-of-bounds reads. On bare-metal or RTOS targets without memory protection, the adjacent byte could be exposed or influence whether a path was accepted, and instrumented builds could crash. This issue is fixed in version 7.22.	6.5	Details
CVE-2026-120634	CGI::Carp versions before 5.00 for Perl leak warnings across requests in persistent environments via the warningsToBrowser buffer. Warnings are held in a package-level buffer until warningsToBrowser writes them into the page as HTML comments, and the buffer is never cleared between requests. Under mod_perl, FastCGI or PSGI, warnings from one request are written into a later one. Warnings that contain one user's request data can appear in the HTML sent to another user.	6.5	More Details
CVE-2026-103917	The The Quiz and Survey Master (QSM) – Quiz Maker & Survey Maker plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 11.2.7. 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 submission nonce is dispensed to any unauthenticated caller by the public wp_ajax_nopriv_qsm_create_quiz_nonce endpoint, meaning it functions as a CSRF token rather than an authorization barrier and imposes no meaningful obstacle to exploitation.	6.5	More Details
CVE-2026-123464	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Liquid Web / StellarWP The Events Calendar the-events-calendar allows Stored XSS.This issue affects The Events Calendar: from n/a through 6.18.3.	6.5	More Details
CVE-2026-119510	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Saeed MC Woocommerce Wishlist smart-wishlist-for-more-convert allows Stored XSS.This issue affects MC Woocommerce Wishlist: from n/a through 2.0.3.	6.5	More Details
CVE-2026-120632	CGI versions before 5.00 for Perl allow CPU exhaustion via a backtracking regex on the XForms multipart/related Content-Type. When a POST Content-Type contains multipart/related, the boundary and start parameters are extracted with an unanchored pattern that puts .+ on either side of the boundary capture, which backtracks in cubic time on a header that does not match. No request body is needed.	6.5	More Details
CVE-2026-21850	HCL AION is affected by a vulnerability where user-controlled input could be included in HTTP response headers without proper neutralization of CR/LF characters. This may allow an attacker to inject headers or split responses, potentially resulting in unintended behavior or security impact under certain conditions.	6.5	More Details
CVE-2026-123485	Ground Station from 0.6.0 before 0.8.20 does not restrict the get-orbital-sources Socket.IO handler (also exposed as get-tle-sources) to administrators, although the orbital-source write handlers are admin-only. An authenticated operator-role user can call either handler to retrieve the plaintext usernames, passwords, and tokens that administrators stored for basic and token orbital sources.	6.5	More Details
CVE-2026-35495	In IMS stack, improper handling of SIP packets leads to Incorrect_Access_Control vulnerability	6.5	More Details
CVE-2026-115952	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPMU DEV Forminator forminator allows Stored XSS.This issue affects Forminator: from n/a through 1.58.3.	6.5	More Details
CVE-2026-97848	A flaw was found in the token sanitization logic of Keycloak, an open source identity and access management solution. The issue occurs when a protocol mapper is configured to emit structured claims using the JSON type. The security check designed to remove unauthorized role mappings only looks for standard Java maps and fails to recognize Jackson based JSON objects. This allows an attacker to inject forged client roles into security tokens, which could lead to unauthorized access to protected resources.	6.5	More Details
CVE-2026-121969	netrek-client-cow through 3.3.3 contains a stack-based buffer overflow vulnerability in handleSMessage() in short.c that allows malicious servers to overflow a 100-byte stack buffer by sending oversized SP_S_MESSAGE packets. A malicious Netrek server or man-in-the-middle on the plaintext TCP connection can send overlong or unterminated message bodies to write server-controlled bytes onto the stack and crash the client.	6.5	More Details
CVE-2026-121968	Netrek-client-cow through 3.3.3 contains an out-of-bounds read vulnerability in short.c handleSMessage() that allows malicious servers to crash clients via an unchecked m_recpt index. Attackers controlling a Netrek server or intercepting the plaintext TCP connection can send SP_S_MESSAGE packets with m_recpt of 36 or more, reading past players[] and shipnos to deny service.	6.5	More Details
CVE-2026-112072	vault-java-driver, a Java client for HashiCorp Vault, parses Vault's JSON responses with a vendored minimal-json parser that has no nesting depth limit. A deeply nested value raises a StackOverflowError, which escapes catch (Exception) handlers and kills the reading thread. A Vault token that can write but not read a KV v2 path can store such a value there, so every later read of that path through the driver fails. This requires Vault 1.19.x or earlier, because 1.20 and later reject values nested deeper than 298 levels. This issue affects io.github.jopenlibs:vault-java-driver 5.2.0 through 6.2.3 and is fixed in 7.0.0.	6.5	More Details
CVE-2026-119520	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Brainstorm Force Spectra ultimate-addons-for-gutenberg allows Stored XSS.This issue affects Spectra: from n/a through 2.20.4.	6.5	More Details
	The Everest Forms – Contact Form, Payment Form, Quiz, Survey & Custom Form Builder with AI plugin for		

CVE-2026-89101	WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 3.6.2 via the get_entry due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with custom-level access and above, to view, read, and permanently delete forms and entries belonging to any other user — including personally identifiable information submitted through public contact and lead forms — regardless of form ownership.	6.5	More Details
CVE-2026-107773	The Dokan: AI Powered WooCommerce Multivendor Marketplace Solution WordPress plugin before 5.3.3 does not correctly verify authorization when serving a single order and its order notes, allowing unauthenticated attackers to read customer and order information and to add or delete order notes for a subset of orders.	6.5	More Details
CVE-2026-9797	A flaw was found in Keycloak's administrative services (org.keycloak.services.resources.admin). A highly privileged attacker, authenticated with a 'manage-clients' role, could exploit this vulnerability through several methods, including manipulating client JSON Web Key Sets (JWKS), swapping client authenticator types and resetting secrets, or downloading legitimate signing keys. Successful exploitation allows the attacker to obtain a token with 'realm-admin' role assignments, leading to privilege escalation and potential unauthorized access to sensitive resources.	6.5	More Details
CVE-2026-119472	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in David Anderson Redux Framework redux-framework allows Stored XSS.This issue affects Redux Framework: from n/a through 4.5.16.	6.5	More Details
CVE-2026-120850	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Elementor Elementor Website Builder elementor allows Stored XSS.This issue affects Elementor Website Builder: from n/a through 4.3.5.	6.5	More Details
CVE-2026-85737	Velociraptor is a tool for collecting host-based state information using Velociraptor Query Language (VQL) queries. Prior to 0.77.2, SQLPlugin.Call in vql/parsers/sql/sql.go does not enforce plugin-level FILESYSTEM_READ or NETWORK checks before the mysql and postgres branches pass a caller-controlled connstring to sql.Open, allowing arbitrary outbound database connections. With attacker-controlled MySQL connection options that enable local-infile access, a rogue MySQL server can request files readable by the Velociraptor server process, including root-readable files when that process runs as root. The SQLite file accessor still enforces FILESYSTEM_READ, but a low-privilege analyst with ANY_QUERY can use the zero-permission data accessor and ATTACH DATABASE to create files without the plugin-level check. This issue is fixed in version 0.77.2.	6.5	More Details
CVE-2026-112341	Wazuh versions from 4.0.0 before 4.14.9 contain a sql injection vulnerability in WazuhDBBackend._substitute_params due to sequential regex placeholder cross-contamination. Authenticated users with agent:read on one agent can inject UNION SELECT via the q and search parameters to extract every agent's internal_key through a blind boolean oracle on total_affected_items.	6.5	More Details
CVE-2026-54383	VitaFit cloud API before 2026-10-30 contained an excessive data exposure vulnerability that allows any authenticated user to query the GET /front/relation/search/ endpoint and retrieve PII and health-related profile information for user records. Attackers can enumerate the user directory using overlapping alphanumeric search terms to harvest identifiers, emails, birthdays, gender, height, weight goals, phone numbers, and Firebase UIDs.	6.5	More Details
CVE-2026-120640	CGI versions before 5.00 for Perl allow the POSTDATA, PUTDATA, PATCHDATA and XForms:Model parameters to be set from the query string or form fields. CGI stores a non-form request body under POSTDATA, PUTDATA or PATCHDATA, and an XForms body under XForms:Model, but also accepts these names from the query string, a form field or a multipart part, so an application cannot tell a client-sent value from the real body. A cross-site HTML form can post POSTDATA={"admin":true} to an endpoint that reads JSON from param('POSTDATA'), a request forgery that needs no CORS preflight.	6.5	More Details
CVE-2026-96547	A flaw was found in the Dynamic Client Registration component of Keycloak, an open-source identity and access management solution. The issue occurs because the system does not properly restrict which claim names can be used when setting up new clients. An attacker with valid registration credentials could create a client that incorrectly maps standard user profile information to sensitive security roles, potentially allowing them to gain unauthorized privileges on external applications that trust Keycloak tokens.	6.5	More Details
CVE-2026-119500	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bPlugins Flash & HTML5 Video html5-video-player allows Stored XSS.This issue affects Flash & HTML5 Video: from n/a through 2.14.1.	6.5	More Details
CVE-2026-93779	The Tutor LMS – eLearning and online course solution plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 4.1.2 via the init_routes due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with subscriber-level access and above, to read paid course lesson and topic content without enrollment, retrieve quiz answer keys including the is_correct field before attempting a quiz, and enumerate the email addresses, usernames, and registration data of other users including instructors and administrators. Exploitation requires that the attacker hold a valid Tutor LMS API key/secret pair, which is issued to subscriber-level users through the plugin's API key management feature.	6.5	More Details
CVE-2026-19131	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow low-privileged users to query arbitrary indices and read sensitive data due to missing authorization.	6.5	More Details
CVE-2026-	GodotSteam 4.17 through 4.23.2 trusts the peer value of 1 to mean that a player is the server. A	6.5	More

123017	grant_gold(1000000) call can be forged.		Details
CVE-2026-120845	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPMU DEV Smush Image Compression and Optimization wp-smushit allows Stored XSS.This issue affects Smush Image Compression and Optimization: from n/a through 4.3.5.	6.5	More Details
CVE-2026-63437	2FAuth is a web app to manage Two-Factor Authentication (2FA) accounts and generate their security codes. Prior to 8.0.0, the recipients() method in app/Api/v1/Controllers/TwoFAccountShareController.php receives a caller-selected TwoFAccount through Laravel model binding but does not call the manageShares authorization policy before listing its recipients. When account sharing is enabled, an authenticated user can call GET /api/v1/twofaccounts/{victimId}/recipients for accounts owned by other users, enumerate registered user IDs and display names, test exact email addresses with filter[nameOrEmail], and inspect each account's sharing relationships. This issue is fixed in version 8.0.0.	6.5	More Details
CVE-2026-87044	The Mbed TLS crypto shim driver in drivers/crypto/crypto_mbedtls_shim.c drives PSA multipart cipher and AEAD operations. In mbedtls_cbc() and mbedtls_aead(), every error path after a successful psa_cipher_encrypt_setup() / psa_aead_decrypt_setup() returned directly without calling psa_cipher_abort() / psa_aead_abort(). Because the abort is the only thing that reaches mbedtls_cipher_free(), each failed operation permanently leaked the heap-allocated mbedtls_aes_context (roughly 288 bytes) that setup had allocated from Mbed TLS's fixed static heap (_mbedtls_heap[CONFIG_MBEDTLS_HEAP_SIZE], default 512 bytes). With CONFIG_PSA_CRYPTO_PROVIDER_TFM the leaked object is instead a finite secure-partition multipart-operation slot. The failure is chosen by an unauthenticated attacker. With CONFIG_NET_L2_IEEE802154_SECURITY backed by this driver, ieee802154_decrypt_auth() in subsys/net/l2/ieee802154/ieee802154_security.c invokes cipher_ccm_op() on every received secured frame, with no authentication ahead of the MIC check. A device in radio range can transmit a stream of syntactically valid 802.15.4 frames carrying a bogus MIC; each one makes psa_aead_verify() fail and leaks a block. The CBC path is reachable the same way through the OSDP secure channel, where CONFIG_OSDP_SC_ENABLED selects this shim and osdp_encrypt() / osdp_decrypt() leave out_buf_max unset, so every operation fails inside psa_cipher_update(). Exhausting the Mbed TLS heap — which the default configuration reaches after a couple of failed operations, and any realistic configuration reaches in well under a second of frames — makes all subsequent mbedtls_calloc() calls fail. Every later cryptographic operation in the image then fails permanently, including link-layer security and any TLS/DTLS sharing the same heap, until the device is rebooted. There is no memory corruption or information disclosure: frames with an invalid MIC are still rejected, so the impact is limited to availability. The fix routes all post-setup failures in mbedtls_cbc() and mbedtls_aead() through a common error: label that calls the matching PSA abort before returning. Setup failures need no change, since the PSA core aborts the operation itself when setup fails.	6.5	More Details
CVE-2026-120650	CGI versions before 5.00 for Perl allow memory, CPU and disk exhaustion via missing or unenforced request size, parameter and upload limits. $CGI::POST_MAX defaults to no limit, and when set is not enforced for chunked multipart bodies or for the boundary line of a multipart body without a boundary= parameter. Bodies saved as PUTDATA, POSTDATA or PATCHDATA uploads are read into memory in one go, and nothing limits the number of parameters or uploads.	6.5	More Details
CVE-2026-122053	The Symfony Serializer component ObjectNormalizer treats any attribute name containing . (and, from Symfony 6.4, []) as a writable property path, allowing untrusted input to modify properties of nested objects and bypass their #[Ignore] metadata attribute in Symfony versions 5.4.41 prior to 5.4.56, 6.4.9 prior to 6.4.50, 7.0.9 prior to 7.1.0, 7.1.2 prior to 7.4.23, and 8.x prior to 8.1.11. ObjectNormalizer::isAllowedAttribute() accepts such names, and setAttributeValue() hands the name straight to PropertyAccessor::setValue(), which parses it as a property path and traverses into the nested object. A payload key such as customer.admin writes to $order->customer->admin. The #[Ignore] metadata attribute is only consulted when the nested object is denormalized in its own right, never when it is reached through a path. #[Groups] restrictions are not bypassed: the path is only accepted when no groups are passed in the context, and then groups restrict nothing. When the root class carries neither #[Ignore] nor #[Groups], no allowlist applies and every key of the payload is let through. Because PropertyAccessor also resolves a path segment against public methods, a segment matching a public method name invokes that method with the attacker’s value.Applications that bind untrusted input to objects are affected, including controllers using #[MapRequestPayload] or #[MapQueryString], whose default normalizer is ObjectNormalizer. With OBJECT_TO_POPULATE, as used for partial updates, the traversal reaches an already hydrated entity graph, and the modified field may be persisted. The fix accepts a property path only when the class metadata declares an attribute of that exact name. Declared paths keep working unchanged, and a path in the payload with no matching declaration is ignored.	6.5	More Details
CVE-2026-110534	The Redux Framework plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'content' parameter in all versions up to, and including, 4.5.16 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 target site's theme to register a color_scheme field on the user profile via Redux_Users::set_profile(), which causes the nonce to be rendered on /wp-admin/profile.php for every logged-in user, making it accessible to Subscribers.	6.4	More Details
CVE-2026-	The Image Hover Effects Ultimate Visual Composer (Flipbox - Awesomes Flip Boxes Image Overlay) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'flip-box-image-upload-url-01-alt' parameter in versions up to, and including, 3.1.1. This is due to the plugin saving the image-alt field through sanitize_text_field() in Inc/Style22::register_child() (and Inc/Style18, 19, 20, 25, 29) — which preserves the double-quote character — and then concatenating the stored value into a double-quoted HTML attribute in Public_Render/Style22::default_render() (and the corresponding Style18/19/20/25/29 renderers) with no esc_attr()	6.4	More Details

109973	escaping. This makes it possible for authenticated attackers, with contributor-level access and above (when an administrator has delegated the plugin's 'Who can edit' capability via the plugin Settings page, or on multisite installations where even administrators lack unfiltered_html), to inject arbitrary web scripts in pages that will execute whenever a user accesses any page containing an affected [oxilab_flip_box] shortcode or block.		
CVE-2026-97642	The Wp Parsidate plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the calendar Gutenberg block's 'theme' attribute in versions up to, and including, 6.4. This is due to insufficient input sanitization and output escaping on the block attribute value which is concatenated directly into an HTML class attribute in the printCalendar() function without esc_attr(). This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-119098	The LifterLMS – WP LMS for eLearning, Online Courses, & Quizzes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'answer[]' parameter in all versions up to, and including, 10.3.2 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. Exploitation requires the attacker to be enrolled as a student in a course containing a Content-type quiz question; the injected payload executes in the administrator's browser session during the normal grading workflow when 'Start a Review' is clicked on the affected attempt.	6.4	More Details
CVE-2026-119165	The WPBakery Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'display_name / nickname' parameter in all versions up to, and including, 9.0.1 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. Successful execution requires that at least one public post attributed to the attacker's account be rendered through a Basic Grid using a Grid Builder template with the Post Author element configured to link to the post author; Author-level users can satisfy this precondition unassisted, while Subscribers depend on an administrator having assigned or published a post under their account.	6.4	More Details
CVE-2026-104719	The CookieYes WordPress plugin before 3.5.8 does not correctly restrict who can write its cookie-category script fields, and does not sanitize or escape them, allowing users with the Contributor role to store JavaScript that executes in the browsers of site visitors and of an administrator reviewing the content.	6.4	More Details
CVE-2026-121519	The Social Slider Feed – Social Media Feed & Gallery Widgets plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'slidespeed' parameter in all versions up to, and including, 2.3.8 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. The missing current_user_can() check in the Factory framework's connect() dispatcher allows Subscriber-level users to bypass the manage_options capability gate and both harvest a valid wis_edit_feed nonce and overwrite any feed's slidespeed setting, after which the stored payload fires on every public pageview embedding the feed shortcode.	6.4	More Details
CVE-2026-120532	The wpForo Forum plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'post[body]' parameter in all versions up to, and including, 3.2.2 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.	6.4	More Details
CVE-2026-96565	The WP-Members Membership Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via WooCommerce Checkout Multicheckbox/Multiselect Field (scalar bypass of wpmem_sanitize_array) in all versions up to, and including, 3.5.7 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 only exploitable via the WooCommerce classic checkout path, as the sibling registration, profile, and account-edit handlers implode the value before sanitization, which raises a PHP 8 TypeError on scalar input and fails closed.	6.4	More Details
CVE-2026-104812	The Redux Framework plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'multi_media' Field Array Key in all versions 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 wp_kses_post sanitization applied at save time operates only on array leaf values, leaving array keys entirely unsanitized; the injected key is then rendered directly into an id="filelist-<KEY>" HTML attribute without esc_attr() in Redux_Multi_Media::render(), allowing attribute breakout.	6.4	More Details
CVE-2026-102610	fast-agent is a framework for building, running, and evaluating AI agents with Model Context Protocol support. Prior to 0.7.21, fast-agent serve uses HTTP transport bound to 0.0.0.0 on port 8000 without authentication, allowing any network client that can reach the /mcp endpoint to invoke the exposed agent tool. When the server is started with --shell, the agent can call the local execute tool implemented by tools/local_shell_executor.py, so an unauthenticated remote client can cause operating-system commands to run as the server user; without --shell, the client can still consume the operator's model and configured MCP tools. The defaults are defined in cli/commands/serve.py and mcp/server/agent_server.py, and the non-interactive server permission prompt does not prevent the described access. This issue is fixed in version 0.7.21.	6.4	More Details
	The Falang multilanguage for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'falang_term[<taxonomy>][<locale>][<field>] (via order[] driving wp_update_term)' parameter in all versions up		

CVE-2026-118047	to, and including, 1.4.6 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. The exploit is made reliable because the required 'falang' nonce is disclosed to any logged-in user through the equally unprotected wp_ajax_falang_menu_translation handler, requiring no elevated access to obtain.	6.4	More Details
CVE-2026-120533	The Redux Framework plugin for WordPress is vulnerable to Stored Cross-Site Scripting via theme_opts Parameter via User Profile in all versions up to, and including, 4.5.16 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 host theme to have registered a Redux field of a CSS-emitting type (such as link_color, border, or typography) with an output CSS selector, as only the field types 'spinner', 'slider', 'color', and 'date' receive per-type value validation that would block the entity-encoded payload.	6.4	More Details
CVE-2026-120553	The Customer Reviews for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'slides_to_show' parameter in all versions up to, and including, 5.126.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-118050	The Football Pool plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'shouttext' parameter in all versions up to, and including, 2.13.5 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 injected script only fires in the admin Edit view for a shout; the public Shoutbox widget and the admin list view both encode output via Football_Pool_Utils::xssafe(), making the admin Edit view the sole unescaped sink.	6.4	More Details
CVE-2026-116551	The WP Customer Area plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'display_name' parameter in all versions up to, and including, 8.4.0 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.	6.4	More Details
CVE-2026-116545	The All-in-One Video Gallery – Video Player & Galleries for YouTube, Vimeo & Self-Hosted Videos plugin for WordPress is vulnerable to Stored DOM-Based Cross-Site Scripting via the 'custom_fields[].value.label (for key='track')' parameter in all versions up to, and including, 5.0.0 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. Exploitation requires the site's Player Library option to be configured as Plyr/Vidstack (aiovg_player_settings[player]='vidstack') rather than the Video.js default, as the DOM innerHTML sink exists only in the Plyr/Vidstack template path.	6.4	More Details
CVE-2026-120579	The Active Woot Products Tables for WooCommerce. 100% FREE plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'help_title' parameter in all versions up to, and including, 2.1.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-123328	In JetBrains YouTrack before 2026.2.19656 app permission bypass allowed privilege escalation via project tab	6.4	More Details
CVE-2026-91049	The EWWW Image Optimizer WordPress plugin before 8.9.1 does not properly sanitize and restrict a value in post content before using it to dynamically load and execute a script in the page, allowing authenticated attackers with author-level access and above to inject arbitrary web scripts that run in the session of any user who views the affected page, including administrators. This is an incomplete fix of CVE-2026-15446: the origin and path restrictions added from 8.7.4 onward were each bypassable, so versions 8.7.4 through 8.9.0 remain affected.	6.4	More Details
CVE-2026-93900	The Simple CAPTCHA with Cloudflare Turnstile plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' attribute of the [gravity-simple-turnstile] shortcode in versions up to, and including, 1.44.3 This is due to insufficient input sanitization and output escaping on the shortcode attribute in the cfturnstile_gravity_shortcode() function: the value is filtered only by esc_html() and sanitize_text_field() (neither of which touches parentheses or dots) and then emitted via esc_js() in a raw JavaScript expression context outside any string literal (esc_js only escapes quotes, backslashes, and newlines). 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-2026-118784	The WPSpeed plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to, and including, 2.6.10 This is due to a combination of two issues in the LightImages HTML optimizer: (1) Dispatcher::runOptimize() decides whether the current request is the site's home page by comparing only the URL path from REQUEST_URI against the path of the home URL, so on a plain-permalinks install the author archive URL /?author=<ID> is treated as the home page and the LightImages optimizer runs on it; and (2) LightImages::optimize() calls html_entity_decode() across the entire serialized DOMDocument output under the default-enabled img_processing_entity_decode setting, converting any entity-encoded markup present as plain text in the page (including WordPress's rendered author title) into live HTML. This makes it possible for authenticated attackers, with Subscriber-level access and above, to store entity-encoded markup in their own nickname/display_name through the normal profile endpoint and have that markup rehydrated into executing	6.4	More Details

	script when any logged-out visitor loads their author archive.		
CVE-2026-17372	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to probe internal network resources due to insufficient validation of webhook destination URLs. User-configured webhook addresses are not sufficiently restricted, so the server could be made to contact internal systems.	6.4	More Details
CVE-2026-120550	The WP User Manager – Registration Form, Login Form, User Profile Builder & Member Directory plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'name (REST users endpoint) -> wp_users.display_name' parameter in all versions up to, and including, 2.10.2 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. The payload is stored via the WordPress core REST endpoint POST /wp-json/wp/v2/users/me, which bypasses the plugin's own wpum_sanitize_text sanitizer applied on its front-end account form, making the save-time sanitization ineffective as a mitigation.	6.4	More Details
CVE-2026-17238	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information from other tenants due to path parameter injection. Values in the request path are not sufficiently validated, which could allow access to data belonging to other tenants.	6.4	More Details
CVE-2026-122059	The WP ImageViewer plugin for WordPress is vulnerable to Stored DOM-Based Cross-Site Scripting via the 'img.alt' parameter in all versions up to, and including, 3.0.2 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 a front-end content plugin such as bbPress to be active, as it grants Subscriber-level users the bbp_participant capability needed to publish image-bearing content containing the encoded payload. Exploitation by attackers with contributor-level access and above requires that the site allows Contributors (or higher) to submit image HTML in post content — the WordPress default. On a default installation, where that is not configured, the vulnerability requires attackers with custom-level access and above.	6.4	More Details
CVE-2026-121976	The Modula plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'items' parameter in versions up to, and including, 3.0.17 This is due to insufficient input sanitization of the per-image 'link' field in the save_merged_items() REST handler and Images\Adapter::normalize_item_row(), which preserves unknown keys verbatim, combined with output escaping in Modula_Helper::generate_attributes() that applies only esc_attr() to the resulting anchor href and does not strip the 'javascript:' URL scheme. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page and clicks the gallery tile.	6.4	More Details
CVE-2026-93902	The Soledad theme for WordPress is vulnerable to Stored Cross-Site Scripting via Social Profile Fields in all versions up to, and including, 8.7.7 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 injected payload is scoped to the attacker's own user meta but is exposed publicly on their author archive page at /author/<slug>/, which is accessible to unauthenticated visitors regardless of whether the attacker has published any posts.	6.4	More Details
CVE-2026-9601	The Stackable – Page Builder Gutenberg Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'update_block_style' endpoint in all versions up to, and including, 3.19.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-118800	The aBlocks – Gutenberg Blocks, User Dashboard Builder, Popup Builder, Form Builder & Animation Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'headingTag' parameter in all versions up to, and including, 2.18.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-118204	The WP Data Access – App Builder for Tables, Forms, Dashboards, Charts & Maps plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'ImageURL column value (populated from wp_usermeta.description in the demonstrated path)' parameter in all versions up to, and including, 5.5.89 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. Exploitation requires an administrator to have published a DataTables shortcode over a database column the attacker controls (e.g., wp_usermeta.description) with the Image URL media type assigned to that column — both are supported plugin features but are not enabled by default.	6.4	More Details
CVE-2026-118048	The WP Data Access plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Simple Form autocomplete lookup label in versions up to, and including, 5.5.89 This is due to insufficient output escaping on the value returned by WPDA_Autocomplete::autocomplete_lookup() when it is emitted into a single-quoted HTML attribute by WPDA_Simple_Form_Item_Autocomplete::show_item() (the escape-output lint is explicitly suppressed on the echo line). This makes it possible for authenticated attackers, with Subscriber-level access and above, who are permitted to edit a lookup row through a legacy Form, to inject arbitrary web scripts in pages that will execute whenever a user — including a higher-privileged user editing a linked record that uses the autocomplete relationship — accesses the injected page.	6.4	More Details

CVE-2026-116621	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 'pm_note (any custom Textarea metakey with html disabled)' parameter in all versions up to, and including, 2.14.1 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. Successful exploitation requires a privileged victim to click the attacker-rendered anchor on the target profile page, which triggers the DOM gadget that concatenates the unescaped data-src value into an HTML string passed to jQuery.	6.4	More Details
CVE-2026-17237	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to server-side request forgery.	6.4	More Details
CVE-2026-120479	The WP Data Access – App Builder for Tables, Forms, Dashboards, Charts & Maps plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Data Projects front-end simple form in versions up to, and including, 5.5.90 This is due to insufficient input sanitization and output escaping on the value of TEXT/TINYTEXT/MEDIUMTEXT/LONGTEXT columns rendered by the WPDA_Simple_Form_Item_Textarea::show_item() method, which emits the stored column value directly inside a <textarea> element after only replacing '&' with '&'. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-118046	The JS Help Desk – AI-Powered Support & Ticketing System plugin for WordPress is vulnerable to Stored DOM-Based Cross-Site Scripting via the 'jsticket_message' parameter in all versions up to, and including, 5.0.2 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. The payload fires specifically when an administrator or agent opens the affected ticket and the page initializes VenoBox, which reads the browser-decoded data-title attribute and passes it to jQuery .html(), making routine ticket review the trigger condition.	6.4	More Details
CVE-2026-116562	The Motors – Car Dealership & Classified Listings Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'stm_f_s[make]' parameter in all versions up to, and including, 1.4.128 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 Free Listing Submission feature to be enabled, which is shipped on by default via the Setup Wizard demo configuration.	6.4	More Details
CVE-2026-17236	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to improper authorization. Authorization checks are not applied when certain organization URLs are resolved, which could allow access to information belonging to others.	6.4	More Details
CVE-2026-17233	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain information about internal network services due to improper validation of user-supplied URLs. Addresses supplied by users are not sufficiently restricted, so the server could be made to contact internal systems.	6.4	More Details
CVE-2026-118189	The Posts Table with Search & Sort plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'date_format' parameter in all versions up to, and including, 1.4.14 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The payload bypasses wp_kses_post at save time because it contains no literal angle bracket characters; the malicious HTML tags are only reconstructed at render time, making this exploitable by Contributors who would ordinarily lack the unfiltered_html capability.	6.4	More Details
CVE-2026-107124	A flaw was found in the OIDC logout endpoint of the keycloak-services component, which handles user session termination in Red Hat Build of Keycloak. The issue occurs because the system sets a session cookie based on an unvalidated token hint before completing security checks. An attacker can use this flaw to fix a session ID in a victim's browser, allowing them to hijack the victim's subsequent login and gain full control over their account.	6.4	More Details
CVE-2026-120671	The UsersWP – Front-end login form, User Registration, User Profile & Members Directory plugin for WP plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'badge' parameter in all versions up to, and including, 1.2.80 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The exploit is particularly effective against higher-privileged users — such as editors and administrators — who preview a Contributor's pending post containing the malicious shortcode.	6.4	More Details
CVE-2026-115816	The Kubio AI Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'comment (review body)' parameter in all versions up to, and including, 2.9.4 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's review containing the payload to be approved, either automatically (due to a previously approved review from the same account) or manually by an administrator, and the active single-product template must use a Kubio-rendered wp:post-content block.	6.4	More Details

CVE-2026-17395	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to access internal network resources due to improper validation of a user-supplied URL. Destinations are not sufficiently restricted, which could allow the server to be made to contact internal systems.	6.4	More Details
CVE-2026-118054	The LearnPress – Course Review plugin for WordPress is vulnerable to Stored DOM-Based Cross-Site Scripting via the 'review_title (inside `data.args.review_title`)' parameter in all versions up to, and including, 4.2.2 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. The injected payload only executes after an administrator approves the submitted review, though sites with comment_previously_approved auto-approval configured may bypass manual moderation.	6.4	More Details
CVE-2026-17390	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow an authenticated user to execute arbitrary JavaScript in the web UI due to cross-site scripting. This could alter the intended functionality of the page and potentially lead to credential disclosure within a trusted session.	6.4	More Details
CVE-2026-17304	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to improper input validation. Locations supplied when service definitions are imported are not sufficiently validated, which could allow the server to retrieve content it should not access.	6.4	More Details
CVE-2026-104760	The weDocs: AI Powered Knowledge Base, Docs, Documentation, Wiki & AI Chatbot plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'modalPlaceholder' Block Attribute in all versions up to, and including, 2.6.1 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. Because Contributors can save posts in pending status, a malicious payload in the modalPlaceholder block attribute will execute in the browser of any admin or editor who previews or views the pending post.	6.4	More Details
CVE-2026-114431	The Enable Media Replace WordPress plugin before 4.2.3 does not pass a replaced media file through the WordPress upload pipeline, so the upload prefilter that SVG-sanitizer Enable Media Replace WordPress plugin before 4.2.3 rely on never runs, allowing an authenticated user with upload access to store an SVG file containing script that executes when the file is opened directly. It requires an SVG-enabling Enable Media Replace WordPress plugin before 4.2.3 to be active, as the replace path otherwise rejects SVG uploads.	6.4	More Details
CVE-2026-97367	A flaw was found in the Keycloak Account REST API where it incorrectly handles session identification. A malicious client owner can manipulate their own security tokens to point to a different user's active session. This allows the attacker to access and modify the victim's account information, potentially leading to a full account takeover by changing the recovery email and resetting the password.	6.4	More Details
CVE-2026-17370	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain an access token for another user due to improper authentication. The sign-in flow does not sufficiently verify the identity of the user completing it, which could allow another user's identity to be assumed.	6.4	More Details
CVE-2026-17317	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to access internal resources and cause a denial of service due to server-side request forgery.	6.4	More Details
CVE-2026-122222	The Permalink Manager Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'slug' parameter in all versions up to, and including, 2.6.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. An Author-level attacker can submit a percent-encoded HTML/JavaScript payload as a post slug via the REST API, which survives sanitization intact and executes in an administrator's browser session when the URI Editor admin page is loaded.	6.4	More Details
CVE-2026-120515	The SEOPress – AI SEO Plugin & On-site SEO plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'seopress_google_analytics_affiliate_tracking' and 'seopress_google_analytics_download_tracking' settings in versions up to, and including, 10.3. This is due to insufficient input sanitization and output escaping on these settings as they are interpolated into the inline Google Analytics tracking snippet by seopress_google_analytics_js(): the affiliate value receives no sanitization at all (it is omitted from inc/admin/sanitize/Sanitize.php) and lands inside a <script> block, while the download value is only passed through sanitize_text_field() and lands inside a JavaScript regular-expression literal that preserves parentheses, semicolons and slashes. This makes it possible for authenticated attackers, with Subscriber-level access and above (where an administrator has delegated the SEOPress 'analytics' capability under Settings > Advanced > Security — the precondition Wordfence accepted for CVE-2026-101357), to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-17303	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to access internal network resources due to improper validation of a user-supplied URL. The address is not sufficiently restricted, which could allow the server to contact internal systems.	6.4	More Details
CVE-2026-119484	Cross-Site Request Forgery (CSRF) vulnerability in Supsystic Photo Gallery by Supsystic gallery-by-supsystic allows Cross Site Request Forgery.This issue affects Photo Gallery by Supsystic: from n/a through 1.21.6.	6.3	More Details

CVE-2026-89142	In the Wi-Fi NPU FW, there is a possible out-of-bounds write due to an incorrect bounds check. This could lead to local denial of service with user execution privileges needed. User interaction is not needed for exploitation.	6.3	More Details
CVE-2026-122188	A flaw has been found in DeepGraphLearning KnowledgeGraphEmbedding up to 2e440e0f9c687314d5ff67ead68ce985dc446e3a. Impacted is the function override_config of the file codes/run.py of the component Checkpoint Loading. This manipulation of the argument data_path causes path traversal. 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.	6.3	More Details
CVE-2026-123994	Hisense VIDAA Smart TV firmware V0000.01.00a.P0220 contains an unauthenticated access vulnerability in the DIAL (Discovery and Launch) service on TCP port 56789, which accepts control requests from any LAN-adjacent device without authentication, pairing, or user notification. Attackers can query running application states, enumerate installed applications via HTTP response codes, terminate active sessions with a DELETE request, and launch applications or bypass YouTube's Origin check by spoofing the Origin header to disclose viewing activity and subscriptions or disrupt device functionality.	6.3	More Details
CVE-2026-55649	GeoNode is a geospatial content management system, a platform for the management and publication of geospatial data. Prior to 5.0.3, document abstract metadata is stored without sanitization, allowing a low-privileged remote user to persist arbitrary HTML and JavaScript that executes in another user's browser when the document page is visited. This issue is fixed in version 5.0.3.	6.3	More Details
CVE-2026-122160	A security vulnerability has been detected in myshell-ai AIlice up to 0.4.0. This vulnerability affects the function LoadModel_PEFT of the file ailice/core/llm/AModelCausalLM.py of the component HuggingFace Model Wrapper. The manipulation of the argument base_model_name_or_path leads to inclusion of functionality from untrusted control sphere. 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-2026-112110	A time-of-check to time-of-use race condition in the SafeNet Authentication Client (SAC) SACSrv log-cleanup function can allow an authenticated, non-administrator local user to redirect a privileged file deletion operation outside the intended log directory. This issue affects SAC releases up to and including 10.9 R3 GA (build 10.9.7449).	6.3	More Details
CVE-2026-108018	The BigFix MCM admin portal is directly accessible from the internet without VPN or network restriction. A client-side configuration file discloses non-sensitive environment details. Exposing the configuration file publicly increases the attack surface and the risk of unauthorized access attempts.	6.3	More Details
CVE-2026-122159	A weakness has been identified in Edge0-AI Audio8_TTS up to 1d64afcc2da56222b41ddcf53de7b8bc54be1fb6. This affects the function ArkTtsRuntime.__init__ of the file onnx_runtime_0_1b_int8/arktts_runtime/runtime.py of the component Model Path Resolution. Executing a manipulation of the argument slow_decode_models can lead to path traversal. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated releases is not disclosed. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-123653	A security vulnerability has been detected in esengine DeepSeek-Reasonix up to 2.52.0. Affected is the function discoverDocs of the file internal/memory/doc.go. The manipulation leads to improper neutralization of input used for llm prompting. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used. Upgrading to version 2.53.0 is able to address this issue. The identifier of the patch is 4ca33493a673c2788aa8598fbca2b2f47a69e1b8. It is suggested to upgrade the affected component.	6.3	More Details
CVE-2026-123308	In JetBrains IntelliJ IDEA before 2026.3 code execution via the document import was possible in untrusted projects	6.3	More Details
CVE-2026-123824	The Symfony Config component XmlUtils::parse() enables DTD validation before rejecting documents that carry a doctype, allowing XML external entity (XXE) injection in Symfony versions prior to 5.4.56, 6.x prior to 6.4.50, 7.x prior to 7.4.23, and 8.x prior to 8.1.11. A remote attacker who can supply XML to this method can determine whether local files exist, cause a denial of service, and, in some configurations, exfiltrate local file content via a crafted XML document whose doctype declares an external file:// entity. XmlUtils::parse() sets $dom->validateOnParse = true before calling loadXML() and only rejects documents carrying a doctype afterwards. Enabling DTD validation makes libxml resolve external entities during loadXML(), and LIBXML_NONET blocks http:// but not file://, so a file:// entity is read from disk before the doctype rejection runs. The content of the file is not returned to the caller, but the distinct libxml error for a missing path reveals whether a file exists, and an entity pointing at a large or slow file causes a denial of service. If the application registers a network-capable stream wrapper such as s3://, a parameter entity can also send the content of a local file to an external server. This is the same issue as CVE-2026-45071, which was fixed in the DomCrawler component but not in Config. Applications are affected if they pass untrusted XML to XmlUtils::parse() directly. The Symfony components that call it process developer-provided or operator-configured sources, such as configuration files and the XLIFF documents fetched by the translation providers.	6.3	More Details
	Solidtime is an open-source time-tracking app. Prior to 0.16.0, TogglDataImporter::importData() read attacker-controlled project id values from projects.json in uploaded ZIP imports and concatenated them into filesystem		

CVE-2026-76806	paths without validation. Because Spatie\TemporaryDirectory\TemporaryDirectory::path() creates missing parent directories, traversal sequences could escape the temporary sandbox and create directories at arbitrary writable host paths. Distinguishable ImportController responses for existing versus missing targets exposed whether suffix-constrained host paths derived from projects_users/{id}.json or tasks/{id}.json existed, because the importer always appended .json. Any registered user able to create an organization and use POST /api/v1/organizations/{org}/import with type=toggl_data_importer could reach the flaw, potentially causing minor availability impact through directory exhaustion and disclosing host layout information. This issue is fixed in version 0.16.0.	6.3	More Details
CVE-2026-123135	A vulnerability was found in langgenius dify up to 1.18.0/2.0.0-beta.2. Affected by this vulnerability is an unknown functionality of the file api/configs/feature/__init__.py of the component Sandbox Run Handler. The manipulation results in hard-coded credentials. The attack can be launched remotely. The exploit has been made public and could be used.	6.3	More Details
CVE-2026-122157	A vulnerability was identified in Purocean Yank Note 3.93.0. Affected by this vulnerability is the function checkPermission of the file src/main/server/index.ts of the component Terminal Handler. Such manipulation leads to os command injection. The attack can be executed remotely. The exploit is publicly available and might be used. Upgrading to version 3.93.1 addresses this issue. The name of the patch is 59f85d48f17a70a402ad59dcecacdbec20f954df. Upgrading the affected component is recommended.	6.3	More Details
CVE-2026-17391	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to broken object-level authorization.	6.3	More Details
CVE-2026-68993	A double free vulnerability in NPU driver due to improper pointer management (940)	6.3	More Details
CVE-2026-122189	A vulnerability has been found in OpenPPL ppl.nn up to bb84dc9952809b3a5a0036858a3d9f68af1c83d5. The affected element is the function OptGraph::InitQuantization of the file src/ppl/nn/engines/cuda/optimizer/opt_graph.cc of the component CUDA Optimizer. Such manipulation of the argument per_channel/bit_width/tensor_max/tensor_min/scale leads to out-of-bounds read. 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 problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-65022	The MDM App Catalog / App Store preview does not properly sanitize or encode user-supplied HTML before rendering it. Injected HTML can be displayed to users who view the preview, which may allow cross-site scripting (XSS) when a user interacts with the crafted content.	6.3	More Details
CVE-2026-122014	A vulnerability has been found in NPC-Worldwide npcpy up to 2.1.27. This affects the function load_sft_model of the file npcpy/ft/sft.py. The manipulation of the argument base_model_name_or_path leads to code injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2026-123322	In JetBrains WebStorm before 2026.3, 2026.2.4 code execution was possible in untrusted projects via the Angular CLI schematics loader	6.3	More Details
CVE-2026-122191	A vulnerability was determined in itsourcecode Airline Reservation System 1.0. This affects an unknown function of the file /admin/manage_booked.php. Executing a manipulation of the argument ID can lead to sql injection. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.	6.3	More Details
CVE-2026-122236	A vulnerability has been found in OpenHands up to 1.24.0. This impacts an unknown function of the component Landing Page. Such manipulation leads to missing authentication. The attack must be carried out from within the local network. The exploit has been disclosed to the public and may be used. Upgrading to version 1.25.0 will fix this issue. The name of the patch is c5efa3ae415def0a903c82d2b17b748e663b1995. Upgrading the affected component is recommended.	6.3	More Details
CVE-2026-49951	RAGFlow before 0.27.0 contains a server-side request forgery vulnerability that allows authenticated attackers to force the server to issue requests to arbitrary internal or external endpoints by supplying an unvalidated base_url to the POST /v1/llm/set_api_key endpoint handled by set_api_key() in api/apps/llm_app.py. Attackers can exploit this flaw to probe shared-network services such as MySQL, Elasticsearch, Redis, MinIO, the Infinity vector database, and cloud metadata endpoints, with raw upstream exception text returned in the response leaking internal service details, open ports, and configuration fingerprints.	6.3	More Details
CVE-2026-123020	A security vulnerability has been detected in eosphoros-ai DB-GPT up to 0.8.1. The affected element is the function FileBasedSkill.get_prompt of the file packages/dbgpt-core/src/dbgpt/agent/skill/claude_skill/__init__.py of the component Jinja2 Template Handler. The manipulation leads to improper neutralization of special elements used in a template engine. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used. Upgrading to version 0.8.2 is sufficient to fix this issue. The identifier of the patch is a9e7a3c026d114fcfb4ffe3eaf78851a636ded16. It is suggested to upgrade the affected component.	6.3	More Details
CVE-2026-	A vulnerability was found in NPC-Worldwide npcpy up to 2.1.27. This vulnerability affects the function get_mlx_response of the file npcpy/gen/response.py of the component MLX Provider. The manipulation of the argument model results in improper input validation. The attack can be launched remotely. The exploit has been	6.3	More Details

122015	made public and could be used.		
CVE-2026-122016	A vulnerability was determined in yangzongzhuan RuoYi-Vue up to 3.9.2. This issue affects the function SysPermissionService.getMenuPermission of the file SysPermissionService.java of the component Permission Service. This manipulation of the argument perms causes improper privilege management. The attack may be initiated remotely. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-121858	The Event Tickets with Ticket Scanner WordPress plugin before 3.2.9 does not properly escape a search value before using it in SQL queries in several of its admin listings, allowing users with access to its admin area (administrators by default, or any role granted access in its settings) to perform SQL injection attacks.	6.3	More Details
CVE-2026-121583	A vulnerability was identified in Sanluan PublicCMS 5. This affects the function TradePaymentService.pendingRefund of the file publiccms-parent/publiccms-trade/src/main/java/com/publiccms/logic/service/trade/TradePaymentService.java. The manipulation of the argument userId leads to authorization bypass. The attack is possible to be carried out remotely. The exploit is publicly available and might be used. The web trade payment controller was removed starting with the 202608 series (commit 7329437).	6.3	More Details
CVE-2026-75598	The Gradle Shadow plugin creates fat or uber JARs and supports file transformation and package relocation. Prior to version 9.6.0, Shadow does not independently validate ZIP entry names before writing them to its output archive. A malicious dependency can cause traversal entry names to be preserved when the applicable archive-processing path does not reject them. Some affected Shadow implementations process dependency archives directly, so upgrading Gradle alone does not universally prevent this behavior. If the resulting archive is extracted without path traversal protection, attacker-controlled files can be written outside the intended destination. This issue is fixed in version 9.6.0.	6.3	More Details
CVE-2026-121927	A vulnerability has been found in InfiniFlow RAGFlow up to 0.27.3. Affected by this issue is the function _account_get of the file common/data_source/seafile_connector.py of the component Seafile Connector. Such manipulation of the argument seafile_url leads to server-side request forgery. The attack can be executed remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-123285	In JetBrains Datalore before 2026.3 command execution was possible in the database task container via JVM options injection	6.3	More Details
CVE-2026-68509	FairEmail is a fully featured, open source, privacy-friendly email app for Android. Prior to 1.2325, shared attachment handling does not adequately sanitize an attacker-controlled filename before constructing its destination path. A local attacker-controlled app can therefore supply path components that escape the intended shared attachment directory and overwrite or corrupt files in the FairEmail private data directory, including account or message databases. Exploitation requires app lock using PIN or biometric authentication and user interaction to unlock FairEmail. This issue is fixed in version 1.2325.	6.3	More Details
CVE-2026-58128	Alan: Health Insurance for Android (com.alanmobile) 1.450.0 contains a path traversal vulnerability that allows a co-resident malicious application to write attacker-controlled files outside the intended directory via the exported ShareReceiverActivity, which uses an unsanitized _display_name value from a shared content URI to construct the destination file path. Attackers can send a crafted ACTION_SEND intent with a _display_name containing directory traversal sequences to overwrite sensitive files within the app's sandbox such as databases, shared_prefs, and WebView data, enabling state tampering or code execution in the app's context without authentication or user interaction.	6.2	More Details
CVE-2026-49405	OpenHuman is an open-source agent harness available as a desktop application and Rust library. Before 0.56.0, the local server exposes the server-sent events endpoint at /events without bearer authentication, permits cross-origin browser access, and uses only a caller-supplied client_id to select WebChannelEvent objects from the process-wide event bus. An unauthenticated local client, or an attacker-hosted web page opened by the victim, can subscribe to another client's stream by supplying a known or guessed identifier; the fixed system identifier makes the proactive-message stream predictable. The exposed events can include complete assistant responses, streamed message content, tool names, tool arguments, and raw tool outputs intended for the local user interface. This issue is fixed in version 0.56.0.	6.2	More Details
CVE-2026-80303	An integer underflow vulnerability in the Avast Windows Filtering Platform (WFP) stream parser on Windows allows denial of service by causing a system crash. The WFP callout driver processes network stream data and computes length values for packet fragment reassembly. The length calculation does not properly validate input stream sizes against expected boundaries. When processing specially crafted input, the length computation underflows, resulting in allocation or buffer access with an extremely large wrapped-around size value. The underflow can be triggered remotely via network traffic destined for the filtered port, or locally via crafted data provided to the filtering interface. The resulting memory allocation failure or out-of-bounds access causes a kernel panic and system crash.	6.2	More Details
CVE-2026-14252	IBM MQ 9.2.0.0 through 9.2.0.44 LTS, 9.3.0.0 through 9.3.0.42 LTS, 9.4.0.0 through 9.4.0.26 LTS, 9.4.0.0 through 9.4.5.1 CD, and 10.0.0.0 through 10.0.0.5 LTS and CD stores potentially sensitive information in log files that could be read by a local user.	6.2	More Details
	A flaw was found in D-Bus. With a privileged Monitoring client attached (for example dbus-monitor or busctl		

CVE-2026-120749	monitor), an unprivileged local user can cause dbus-daemon to abort if a driver-originated broadcast such as NameOwnerChanged or ActivatableServicesChanged cannot be delivered to a recipient (for example due to a deny rule or an exceeded outgoing message queue). Driver broadcasts still use serial 0; when delivery fails, composing the monitor error reply asserts reply_serial != 0 and aborts the daemon.	6.2	More Details
CVE-2026-110021	PLCnext Engineer checks GSDX manifest reference digests but does not cryptographically verify the XML `SignatureValue` over canonicalized `SignedInfo`. An unauthenticated local attacker can modify signed GSDML content, update its manifest digest, retain the public certificate data, and leave an invalid nonempty `SignatureValue`. PLCnext Engineer prior to 2026.6 reports the package as `Valid` and selects the modified device description for import under the default policy.	6.2	More Details
CVE-2026-122309	Kyverno before 1.19.2 contains a denial of service vulnerability that allows namespace-scoped policy authors to exhaust CPU and memory by submitting CEL expressions evaluated without runtime cost limits. Attackers can create a NamespacedValidatingPolicy or NamespacedDeletingPolicy with nested map comprehensions over large ConfigMap fields to OOM-kill Kyverno pods and block cluster-wide admission.	6.2	More Details
CVE-2026-119434	Improper Handling of Highly Compressed Data (Data Amplification) vulnerability in silviucpp ezstd allows an attacker who supplies a zstd frame to ezstd:decompress_using_ddict/2 to exhaust memory and terminate the Erlang VM via a small frame that declares a very large content size. zstd_nif_decompress_using_ddict in c_src/ezstd_nif.cc reads the frame's declared content size with ZSTD_getFrameContentSize and passes it directly to enif_make_new_binary, without the 1 GiB MAX_BUFFER_SIZE check that ezstd:decompress/1 applies before allocating. A valid 65,550-byte frame of RLE blocks declaring 2 GiB is rejected by ezstd:decompress/1 but is fully allocated and decompressed by the dictionary path. The allocation happens inside a NIF, so when it exceeds the memory available to the VM the operating system kills the whole node rather than the calling process. This issue affects ezstd: from 1.0.5 before 1.2.5.	6.2	More Details
CVE-2025-71453	vtenext before 25.02.2 contains a reflected cross-site scripting vulnerability in modules/Home/HomeWidgetBlockList.php that echoes unsanitized widgetId keys from the widgetInfoList JSON parameter. Attackers can induce a logged-in user to submit a crafted POST request with HTML in widgetId keys, executing JavaScript in the victim's vtenext session.	6.1	More Details
CVE-2026-120633	CGI versions before 5.00 for Perl trust the client X-Forwarded-Host header in url, self_url, virtual_host and virtual_port. These take the host name and port from the X-Forwarded-Host request header when present, and otherwise from Host, without validating either. The URLs from url and self_url are the default redirect location and the start_html(-base=>1) base href, and the default start_form action when REQUEST_URI is not set. A client can poison shared caches, and URLs the application stores or sends, with redirects, links and scripts that point at a host it controls.	6.1	More Details
CVE-2026-114627	Web::Simple versions before 0.036 for Perl do not escape values interpolated into double-quoted strings in HTML::Tags output. Under use HTML::Tags or use XML::Tags, a double-quoted string literal becomes a StringThing object that holds each interpolated value as a separate part. The escaping step passes such objects through, and stringify joins their interpolated parts as is. A value passed on its own, as in , $value, , is entity-escaped, but the same value in "Hello $value" is not. An attacker who controls a value that an application interpolates into a double-quoted string can inject script into the generated page.	6.1	More Details
CVE-2026-123203	NEURON (CoreNEURON) through 9.0.2 contains a stack buffer overflow vulnerability that allows attackers to corrupt stack memory by supplying over-long tokens in a crafted model dataset. Attackers can place oversized version or mechanism-name tokens in bbcore_mech.dat, globals.dat, or files.dat loaded by nrniv-core to crash the process.	6.1	More Details
CVE-2026-120421	In Eclipse Mojarra versions 2.2.0 through 4.0.28, 4.1.0 through 4.1.19, and 5.0.0-M1 through 5.0.0-M11, when URL client window mode is enabled (`jakarta.faces.CLIENT_WINDOW_MODE=url`), the client window id from the `jfwid` or `jakarta.faces.ClientWindow` request parameter is appended to generated URLs without URL-encoding. `h:button` renders such a URL into a JavaScript string literal, which allows reflected cross-site scripting. With `com.sun.faces.enableCspNonce=true`, the injected script runs on page load inside the nonce script element, bypassing the Content Security Policy.	6.1	More Details
CVE-2026-120648	CGI versions before 5.00 for Perl allow HTML injection via text containing --> in comment. Arguments are placed between <!-- and --> without escaping, so text containing --> closes the comment early. An application that passes request data to comment can be made to inject HTML into the page.	6.1	More Details
CVE-2026-73472	A flaw was found in GStreamer gst-plugins-good (avidemux). In the superindex and subindex parsers, integer overflow can bypass bounds checks and cause out-of-bounds reads. Because avidemux is auto-plugged by playbin, decodebin, and gst-discoverer, opening or previewing a crafted AVI is sufficient to trigger the issue. Fixed upstream in gst-plugins-good 1.28.6 (GStreamer-SA-2026-0072).	6.1	More Details
CVE-2026-122124	On Yealink UVC40 E2 devices before 319.410.0.71, an attacker with short-term physical access can steal Wi-Fi credentials via the USB interface. Sensitive data within the firmware configuration can be abused to gain root privileges on the device. Within Wi-Fi coverage, the attacker may perform audio and video eavesdropping with no LED alert from the device.	6.1	More Details
CVE-2026-	CGI versions from 4.62 before 5.00 for Perl allow cross-site scripting via a raw apostrophe in URLs returned by url and self_url. Both pass the URL through URI's canonical method, which leaves an apostrophe in the path raw and decodes the %27 that query parameter escaping produces, so an apostrophe in the request path or a parameter	6.1	More

120643	appears raw in the result. An application that places the URL in a single-quoted HTML attribute or JavaScript string is open to cross-site scripting.		Details
CVE-2026-121942	ZBar through 0.23.95 contains an out-of-bounds read vulnerability in _zbar_sq_decode() in zbar/sqcode.c that allows attackers to read heap memory outside the image buffer via crafted SQ code images. Attackers can supply an image with a skewed SQ code finder pattern near the edge, producing unchecked sample coordinates that crash the decoder and leak bytes into output.	6.1	More Details
CVE-2026-122132	go-chi chi 5.2.2 through 5.5.0 contains an open redirect vulnerability in the RedirectSlashes middleware that allows attackers to redirect victims to external hosts by embedding tab characters in request paths. Attackers can craft links with a URL-encoded tab, which browsers strip from the 301 Location header and resolve as a protocol-relative URL, bypassing the fix for CVE-2025-69725.	6.1	More Details
CVE-2026-76419	A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	6.1	More Details
CVE-2026-73471	A flaw was found in GStreamer gst-plugins-good (avidemux). In the Nikon metadata tag parser, a pointer can be dereferenced without verifying that data remains in the buffer, causing out-of-bounds reads. Because avidemux is auto-plugged by playbin, decodebin, and gst-discoverer, opening or previewing a crafted AVI is sufficient to trigger the issue. Fixed upstream in gst-plugins-good 1.28.6 (GStreamer-SA-2026-0072).	6.1	More Details
CVE-2026-115762	draw.io is a configurable diagramming and whiteboarding application. Prior to 31.1.5, the GraphML decoder contains a prototype-pollution vulnerability. Attacker-controlled GraphML reference keys can address inherited object properties, including prototype objects, and the decoder can then assign attacker-controlled attributes to those objects. Importing a malicious GraphML file can trigger client-side prototype pollution. In the advisory-supported cross-site scripting chain, the editor is opened in Trello mode and the user invokes the Trello integration after the import, allowing the polluted state to execute script in the draw.io origin; an existing Trello connection is not required. This vulnerability is fixed in 31.1.5.	6.1	More Details
CVE-2026-110802	Altair is a GraphQL client for all platforms. From 7.2.4 until 8.5.8, packages/altair-iframe-sandbox/src/main.ts reads plugin_sandbox_opts from the iframe-sandbox query string and passes attacker-controlled scriptUrls to injectScript() in packages/altair-core/src/utils/inject.ts, which creates script elements in the page. The intended parent iframe flow places the page in an iframe with sandbox allow-scripts and without allow-same-origin, but direct navigation to a crafted iframe-sandbox URL omits that isolation and executes the supplied script in the origin serving Altair. Exploitation requires a victim to open the crafted URL, and the resulting script can access script-readable storage and make same-origin requests according to the deployment's authentication and cookie controls. This issue is fixed in version 8.5.8.	6.1	More Details
CVE-2026-114229	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') in the Catalog image viewer in Apache OFBiz 24.09 before 24.09.08 on all platforms allows an unauthenticated attacker to execute arbitrary JavaScript in the browser session of a logged-in back-office user via a crafted viewImage URL that the user opens from within the application. Users are recommended to upgrade to version 24.09.08, which fixes this issue.	6.1	More Details
CVE-2026-17232	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote attacker to bypass security restrictions due to improper neutralization of special elements in a request. Specially formed request parameters are not handled safely, which could allow protections to be circumvented.	6.1	More Details
CVE-2026-120636	CGI versions before 5.00 for Perl allow open redirects and script injection via URLs built from REQUEST_URI in url and start_form. url(-absolute=>1), url(-relative=>1) and the default start_form action are built from the client-supplied REQUEST_URI without validation. The result can be protocol-relative (//evil.example), absolute-form (http://evil.example/) or contain backslashes, and url(-relative=>1) can return a javascript: URL. Links and form posts built from these URLs can go to another host.	6.1	More Details
CVE-2026-123622	Usermin through 2.570 contains a cross-site scripting vulnerability in mailbox/detach.cgi that allows remote attackers to execute script by supplying an arbitrary type parameter that bypasses JavaScript filtering. Attackers can email an HTML attachment containing script and lure recipients to a detach.cgi link with type=text/html to run script in the victim's authenticated Usermin session.	6.1	More Details
CVE-2026-88986	Kubeflow Pipelines enables users to build and deploy portable, scalable machine learning workflows. Prior to 2.15.0, the frontend routes /pipeline/k8s/pod and /pipeline/k8s/pod/events use frontend/server/k8s-helper.ts to include untrusted podname and podnamespace query values and backend error details in HTML-capable error responses. An unauthenticated attacker can craft a link that executes JavaScript in the frontend origin when a user who satisfies the deployment's authentication and route-access requirements follows it and reaches an affected response. Cookie disclosure depends on cookie attributes, and server-side code execution or availability impact is not established. This issue is fixed in version 2.15.0.	6.1	More Details
	The QODE Wishlist for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'qode_wishlist_for_woocommerce_guests_items' parameter in all versions up to, and including, 1.2.9 due to		

CVE-2026-121516	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 by guests because the required wp_rest nonce is publicly emitted to unauthenticated visitors on the /wishlist/ page, and the attacker controls the transient key, meaning the payload is stored site-wide and only requires a victim to open a crafted share URL and click the injected title link. Successful exploitation additionally requires an action by an administrator — the attacker cannot trigger the vulnerability on their own.	6.1	More Details
CVE-2026-120638	CGI versions before 5.00 for Perl allow open redirects via HTML entity decoding of the URL after application validation in redirect. redirect decodes HTML entities in its URL before writing the Location header, so a URL the application has already validated can change meaning. For example, //evil.example/ becomes //evil.example/ and sends the user to another host.	6.1	More Details
CVE-2026-76563	Improper neutralization of Script-Related HTML tags in a web page (basic XSS) vulnerability in Fileorbis Informatics Services Trade Inc. Fileorbis allows Using Malicious Files. This issue affects Fileorbis: before 12.5.4.	6.1	More Details
CVE-2026-19876	A reflected cross-site scripting (XSS) vulnerability in the login/SSO error page of INFINITT ULite 5.0.2.1_BN48_20260528 and earlier allows an unauthenticated remote attacker to execute arbitrary JavaScript in the browser of a victim who opens a crafted link. An unsanitized request parameter is reflected without output encoding. Fixed in ULite 5.0.2.1 BN50.	6.1	More Details
CVE-2026-54144	OpenHuman is an open-source agent harness available as a desktop application and Rust library. Before 0.56.0 on macOS, the runtime injected into a supported remote account webview such as Google Meet allows page JavaScript to call getDisplayMedia without a live user gesture. Instead of rejecting the request, the shim falls through to native Chromium capture behavior, and the embedded CEF environment can auto-select the primary display because it lacks the normal desktop-media picker. If OpenHuman already has macOS Screen Recording permission and an attacker obtains JavaScript execution in an allowed embedded origin, the attacker can obtain a real desktop capture stream without a new user gesture. The stream can expose chats, documents, source code, email, meeting content, credentials, one-time codes, and other visible desktop information. The separate direct screen_share_begin_session IPC path failing origin validation does not prevent exploitation through getDisplayMedia. This issue is fixed in version 0.56.0.	6.1	More Details
CVE-2026-123309	In JetBrains IntelliJ IDEA before 2026.3, 2026.2.4 stored XSS was possible on the built-in web server via Markdown preview	6.1	More Details
CVE-2026-121632	Data::MuForm versions through 0.05 for Perl render attribute values and option labels into HTML without escaping. process_attrs writes each attribute value into the markup as is. The select, radio group and checkbox group renderers pass each option to it, so an option's value becomes an unescaped attribute. Option and option group labels are also unescaped, the group label inside a label attribute and the others in element content. Any application whose option list is built from data rather than literals, using an options_<field_name> method, a build_options method or a DBIC model, allows attacker-influenced text in an option value or label that can embed JavaScript in rendered pages. Attribute values built from data, such as through element_attr, are affected the same way.	6.1	More Details
CVE-2026-119616	The Noptin – Newsletter, New Post Notifications & Email Automation plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 4.4.3 via the 'noptin_fields[first_name]' parameter parameter. This makes it possible for unauthenticated attackers to include and execute arbitrary .php files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where .php file types can be uploaded and included. The public Manage Preferences page issues a nonce to unauthenticated visitors, meaning there is no effective authorization barrier — an unauthenticated attacker can store the malicious payload as their first_name and have it executed the next time any newsletter is sent by the site operator. Successful exploitation additionally requires an action by an administrator — the attacker cannot trigger the vulnerability on their own.	5.9	More Details
CVE-2026-122054	Converting crafted BIG-HKSCS input to UCS-4 or the internal wide character encoding, for example with iconv, in the GNU C Library version 2.18 through 2.31 may result in the converter making no progress, causing the calling application to hang.	5.9	More Details
CVE-2026-120415	undici is an HTTP client for Node.js. In versions 7.0.0 through 7.30.1 and 8.0.0 through 8.12.3, the redirect interceptor strips sensitive headers such as Authorization, Cookie, Proxy-Authorization, and Host when a request is redirected to a different origin, but when request headers are supplied as an array of name and value tuples (a valid documented input, for example from Object.entries), the redirect handler misreads them as a flat list so the header names never match and the sensitive headers are not removed. If a header-normalizing interceptor such as cache or deduplicate is composed outside the redirect interceptor, it then serializes the retained headers onto the cross-origin request, disclosing the caller's origin-bound credentials to the unrelated redirect destination. This is a representation-dependent bypass of the cross-origin header stripping added in CVE-2024-30260. The issue is fixed in undici 7.30.2 and 8.12.4, and users should upgrade to one of those versions or later. As a workaround, supply request headers as a plain object or a flat name and value array rather than an array of tuples, or compose the redirect interceptor outside the normalizing interceptor.	5.9	More Details
	The Vanquish Upload Files for WooCommerce plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 2.7.13 via the 'vanupfi_file_name' parameter parameter. This makes it possible for authenticated attackers, with subscriber-level access and above, to read the contents of arbitrary files on the		

CVE-2026-122265	server, which can contain sensitive information. The authorization bypass is achieved by supplying a non-existent order ID (e.g., '.pdf'), which causes wc_get_order() to return false and short-circuits the vanupfi_user_can_access_order_files() check, while the is_pdf() branch selector's loose strpos() substring match allows a traversal payload such as '../.pdf/../../../../wp-config.php' to satisfy the PDF branch and be streamed verbatim via readfile().	5.9	More Details
CVE-2026-92694	FastNetMon is a high-performance DDoS detector and sensor. In version 1.2.9 and earlier, FastNetMon's IPv6 top-talkers screen-draw thread in draw_table_ipv6() in src/fastnetmon_logic.cpp iterates ipv6_host_counters.average_speed_map without holding counter_map_mutex while recalculate_speed() inserts new keys and may rehash the same map. The race requires networks_list to include the targeted IPv6 range. It causes confirmed undefined behavior under load; a process crash is plausible but was not observed, so reliable denial of service has not been established. No fixed release is available as of this review.	5.9	More Details
CVE-2026-116630	undici is an HTTP client for Node.js. In versions 7.0.0 through 7.30.1 and 8.0.0 through 8.12.3, when an Agent composes the redirect and shared cache interceptors, a cached response that is revalidated with a conditional request can be validated by a 304 Not Modified from a different origin. When the origin that stored the response redirects the conditional revalidation request to another origin, the redirect handler strips origin-bound credential headers but not the cache-generated If-None-Match or If-Modified-Since validators, so the redirect destination receives the original origin's validator and undici treats its 304 as successful revalidation of the stored representation. As a result, a shared cache can serve the original origin's stored authenticated response, including one gated by Authorization, to a later unauthenticated caller. The issue is fixed in undici 7.30.2 and 8.12.4, and users should upgrade to one of those versions or later. As a workaround, compose the interceptors as cache then redirect, use per-origin dispatchers and cache stores, or disable shared caching on redirect-capable requests.	5.9	More Details
CVE-2026-112339	Wazuh from 3.9.0 before 4.14.9 contains a missing TLS hostname verification vulnerability in the fluent-forward module's wm_fluent_ssl_ctx() that allows network attackers to impersonate the Fluentd collector by presenting any certificate chaining to the configured ca_file. Attackers who redirect the connection via DNS, ARP, or on-path positions can receive forwarded security telemetry and the shared_key_hexdigest for offline cracking.	5.9	More Details
CVE-2026-122126	reSIProcate reTurn client through 1.14.0 contains a heap buffer overflow in TurnTcpSocket::handleReadHeader(), which TurnTlsSocket inherits, that allows malicious TURN servers or on-path attackers to overwrite memory via oversized frame lengths. Attackers can send STUN or ChannelData frames declaring up to 65535 bytes, writing roughly 57 KB past the fixed 8192-byte mReadBuffer and crashing the client. Only the synchronous TCP and TLS client is affected; the asynchronous client (TurnAsyncSocket) and the reTurn server are not.	5.9	More Details
CVE-2026-112338	Wazuh from 4.3.0 before 4.14.9 contains a server-side request forgery vulnerability in the GitHub module (wm_github.c) that trusts unvalidated Link rel="next" pagination URLs. Attackers controlling the next-page URL can make the manager send requests with the GitHub API token to attacker hosts, exposing organization repositories and settings.	5.9	More Details
CVE-2026-120423	undici is an HTTP client for Node.js. In versions 7.15.0 through 7.30.1 and 8.0.0 through 8.12.3, fetch verifies Subresource Integrity metadata by splitting the integrity string on a single space, but the SRI grammar separates metadata by ASCII whitespace, which also includes the horizontal tab. An integrity value whose digest is preceded by a tab or other ASCII whitespace is parsed as a single unrecognized token and skipped, and when no recognized algorithm remains undici treats the integrity list as empty and accepts the response, so a server returning a body different from the pinned digest passes the check. An application that pins a response with a valid but whitespace-surrounded SRI value receives attacker-controlled bytes with no integrity error, and the attacker needs only to control the response body, not the integrity metadata. The issue is fixed in undici 7.30.2 and 8.12.4, and users should upgrade to one of those versions or later. As a workaround, supply SRI integrity metadata without surrounding whitespace, using a single space to separate multiple digests.	5.9	More Details
CVE-2026-59171	JSON-java is a reference implementation of a JSON package in Java. From version 20150729 through 20260522, JSONTokener.nextSimpleValue can accumulate unbounded numeric tokens before JSONObject.stringToNumber passes them to BigInteger or BigDecimal conversion without a length limit. An application that parses attacker-controlled JSON or XML through JSONObject, JSONArray, or XML.toJSONObject can spend super-linear CPU time converting a sufficiently long numeric literal, blocking request-handling threads and causing denial of service. Strict mode and keep-strings settings in JSONParserConfiguration do not prevent the affected conversion path. Version 20260719 limits numeric conversion length.	5.9	More Details
CVE-2026-77442	Ryot is a self-hosted personal tracking application. Prior to 10.4.0, the createOrUpdateUserIntegration GraphQL mutation in crates/services/user/src/integration_operations.rs allows a low-privileged authenticated user to supply another user's integrationId to create_or_update_user_integration() without an ownership check. SeaORM treats the supplied primary key as an update target, and the operation assigns the caller's user_id while replacing the targeted integration's provider_specifics and other configuration, which can transfer ownership, overwrite configuration, or disable the victim's integration. Exploitation requires obtaining the victim's non-brute-forceable integration id, and the vulnerable update does not disclose existing stored credential values. This issue is fixed in version 10.4.0.	5.9	More Details
CVE-	FileGator is a multi-user file manager. Prior to 7.15.0, POST /upload in backend/Controllers/UploadController.php uses the request-supplied resumableFilename as an unnamespaced key in shared temporary storage. In a multi-user deployment configured with distinct per-user home directories, a low-privileged user with upload permission can set resumableTotalChunks and resumableTotalSize to zero so the assembly loop writes no data, after which		More

2026-94619	the handler reads a pre-existing temporary file with that name, stores it in the attacker's home directory, and removes it. The same filename path can append data when chunks are supplied, allowing disclosure, modification, or deletion of another user's transient object, including a pending archive or the login rate-limit lockfile, while Tmpfs path sanitization limits the primitive to the temporary directory. This issue is fixed in version 7.15.0.	5.9	Details
CVE-2026-123623	Grida through 0.0.24 contains a missing authorization vulnerability in the Forms file-preview API routes that allows unauthenticated attackers to read other organizations' form response files. Attackers can use form and field IDs exposed in public form payloads with a chosen path parameter to obtain service-role signed URLs for attachments and connected Supabase bucket objects.	5.9	More Details
CVE-2026-123287	In JetBrains Datalore before 2026.4 private notebook files could be downloaded without authentication via published interactive reports	5.9	More Details
CVE-2026-77708	A pre-authentication stack-based buffer overflow vulnerability has been identified in the SonicOS TACACS+ authentication client, which in specific conditions could potentially enable a remote unauthenticated attacker to cause an application level denial of service.	5.9	More Details
CVE-2026-120737	The Jupiter X Core plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 4.62.0 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 enumerate and render arbitrary published post types not intended for public listing — including Flamingo CF7 submission records containing submitter names, email addresses, phone numbers, full messages, and IP addresses — and perform meta_query boolean-oracle reads against the postmeta of any published post. Exploitation requires that a Posts or Advanced Posts widget on the site has 'Is Archive Template' enabled, which is the standard Jupiter X archive-template configuration used by most Jupiter X sites; additionally, the nonce verified by the second endpoint is minted via wp_create_nonce and printed on every frontend page as ravenTools.nonce, rendering it ineffective as an authorization barrier.	5.9	More Details
CVE-2026-121963	FreeRDP before 3.32.2 contains a use-after-free vulnerability in the asynchronous dynamic rdpsnd channel that allows malicious RDP servers to trigger freed callback access by closing the channel with queued audio PDUs. Attackers can send a training PDU then close the channel so the playback thread reads the freed callback in rdpsnd_virtual_channel_write, crashing the client.	5.9	More Details
CVE-2026-116574	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to 1.11.2, switch_xml_ampencode() reserved only ten bytes for the widest numeric character reference produced from a four-byte UTF-8 sequence, omitting space for the terminating NUL. When remote-supplied text was serialized at the exact buffer-growth boundary, the terminator wrote one byte beyond the heap allocation. Reachable surfaces include mod_xml_cdr, conference and formatted CDR XML, XML Event Socket output, and XML API output that serializes caller-controlled values. The fixed zero-byte write can abort the process or truncate an adjacent object, while remote code execution has not been demonstrated. This issue is fixed in version 1.11.2.	5.9	More Details
CVE-2026-119746	ProSoft Technology ICX35 devices (X35-HWC-A and ICX35-HWC-E) contain a login lockout bypass in the integrated module web page. The account lockout mechanism that restricts repeated failed authentication attempts is enforced in client-side JavaScript, so a remote attacker can reset the lockout and continue submitting password guesses by deleting the relevant browser cookies, defeating the brute-force protection. This vulnerability has been addressed in version 1.14.158.	5.9	More Details
CVE-2026-121961	FreeRDP before 3.32.2 contains a use-after-free vulnerability in the freerdp-proxy DRDYNVC tracker when intercepting the drdynvc channel. A malicious target server can repeatedly send CREATE_REQUEST_PDU for an active channel id, racing front DATA handling to free a borrowed context and crash the proxy process.	5.9	More Details
CVE-2026-123286	In JetBrains Datalore before 2026.4 improper authorisation allowed read the notebook owner's file storage session token	5.9	More Details
CVE-2026-19126	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information.	5.9	More Details
CVE-2026-77709	A pre-authentication heap-based buffer overflow vulnerability has been identified in the SonicOS TACACS+ authentication client, which in specific conditions could potentially enable a remote unauthenticated attacker to cause an application level denial of service.	5.9	More Details
CVE-2026-110281	IBM Db2 Genius Hub 1.1.2, 1.1.3, 1.1.4, 1.1.5 improperly validates TLS certificate validation, which could allow an attacker to obtain sensitive information using man in the middle technique.	5.9	More Details
CVE-2026-116571	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to 1.11.2, rtmp_rtp2rtmpH264() built an AVC decoder configuration record in a fixed stack buffer by copying wire-derived SPS and PPS values without checking that their sizes and framing fit. An established H.264 call bridged toward an RTMP endpoint could supply oversized SPS and PPS parameter sets and overrun the function's stack frame. The flaw affects only deployments that build and load mod_rtmp and bridge RTP media into an RTMP leg; the module	5.9	More Details

	is disabled in the stock build and configuration. The corruption can abort FreeSWITCH and terminate every active call, and builds without stack protection receive a limited stack-write primitive, although code execution has not been demonstrated. This issue is fixed in version 1.11.2.		
CVE-2026-120222	undici is an HTTP client for Node.js. In versions 7.0.0 through 7.30.1 and 8.0.0 through 8.12.3, when the cache interceptor is composed with a downstream handler that throws during response processing (such as the built-in dump interceptor exceeding its maxSize, or the decompress interceptor rejecting more than five Content-Encoding values), a throw raised asynchronously while a cached response is replayed escapes as an uncaught exception or unhandled promise rejection and terminates the Node.js process. A malicious or compromised HTTP server can crash any such client by serving a cacheable response that triggers the throw on replay, including on a 304 revalidation of a stale entry, so the impact is availability only. The issue is fixed in undici 7.30.2 and 8.12.4, and users should upgrade to one of those versions or later. As a workaround, avoid composing the cache interceptor with a response handler that throws during response processing until upgrading.	5.9	More Details
CVE-2026-123835	In JetBrains Datalore before 2026.4 code execution was possible in another user's computation via an init script upload race condition	5.9	More Details
CVE-2026-63440	2FAuth is a web app to manage Two-Factor Authentication (2FA) accounts and generate their security codes. Prior to 8.0.0, the otpauth image-fetch path validates a hostname through ValidatesUrls::isExternalHost() and then lets IconService::storeRemoteImage() resolve the same hostname again for the HTTP request. When external otpauth image fetching is enabled, an authenticated user controlling low-TTL authoritative DNS can return a public address during validation and an internal address during the later connection, bypassing the private-address deny list to reach loopback, private-network, link-local, or cloud metadata endpoints. This issue is fixed in version 8.0.0.	5.9	More Details
CVE-2026-112938	filelock is a platform-independent file lock for Python. From 3.30.0 until 4.2.1, On POSIX platforms, StrictSoftFileLock and AsyncStrictSoftFileLock validate the coordination directory in _ensure_protocol_directory but later reach the claims directory through _open_directory by pathname, allowing a local account that can rename the coordination name to swap in a symbolic link between check and use during acquisition. That race can create and leave claim files in another writable directory or strand claims in a different strict lock so the second lock times out. Separately, the claims property and force_break follow a resting symbolic link without a race when the lock user inspects or recovers the lock. Claims inspection discloses a file name to the other account only if the resulting exception text or claim_name reaches that account through a shared log, CI output, or error report. A blind force_break recovery that removes live claims from another strict lock can allow two processes into that lock's critical section; this path reaches other strict locks, not arbitrary files. This issue is fixed in version 4.2.1.	5.8	More Details
CVE-2026-17315	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote attacker to obtain sensitive information due to improper validation of user-supplied URLs.	5.8	More Details
CVE-2026-88979	Kubeflow Pipelines enables users to build and deploy portable, scalable machine learning workflows. From 2.17.0 until 2.18.0, the TensorBoard proxy token introduced by the incomplete remediation for CVE-2026-54745 uses MINIO_SECRET_KEY as its HMAC secret, whose bundled default is publicly known. In an authorization-disabled deployment using that default, an unauthenticated attacker can forge a token containing a chosen viewerName and namespace; the proxy constructs the destination from the viewerName plus the -service suffix, the namespace, and the configured cluster domain, then reads responses on port 80 under the /tensorboard/<viewer>/ path. Resource-name validation and path-traversal rejection remain enforced, authorization-enabled deployments still check access to the selected namespace, and unrestricted metadata access, writes, or service disruption are not established. This issue is fixed in version 2.18.0.	5.8	More Details
CVE-2026-112243	The Duplicator WordPress plugin before 5.1.0, duplicator-pro WordPress plugin before 5.1.0 does not sanitise and escape a parameter before reflecting it on one of its administrative pages in certain configurations, leading to Reflected Cross-Site Scripting that executes in the session of a logged-in administrator who is tricked into opening a crafted link.	5.8	More Details
CVE-2026-16710	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to a server-side request forgery vulnerability.	5.8	More Details
CVE-2026-17306	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote attacker to obtain sensitive information from internal network resources due to server-side request forgery.	5.8	More Details
CVE-2026-97373	draw.io is a configurable diagramming and whiteboarding application. Prior to 30.3.8, the optional /proxy endpoint contains an incomplete server-side request forgery blocklist. When the endpoint is enabled, the URL validator does not reject the RFC 6598 shared address range 100.64.0.0/10. An unauthenticated remote attacker can cause the draw.io server to request internal services that are reachable in this range, potentially disclosing data from Carrier-Grade NAT, Kubernetes, cloud, or overlay-network addresses. This vulnerability is fixed in 30.3.8.	5.8	More Details
CVE-2026-122140	Trawl 1.5.0 before 1.10.0 contains a server-side request forgery vulnerability that allows unauthenticated attackers to bypass the MCP outbound URL policy using IPv4-mapped IPv6 addresses. Attackers can supply hex-normalized addresses like ::ffff:7f00:1 directly or via redirects to fetch loopback, private, and cloud metadata services and read responses.	5.8	More Details

CVE-2026-103932	ModSecurity is an open source, cross platform web application firewall (WAF) engine for Apache, IIS and Nginx. From 3.0.5 until 3.0.17, the PCRE2 implementation of @rxGlobal in src/utils/regex.cc converts pcre2_match match-limit errors into an ordinary no-match result instead of propagating a non-OK RegexResult. When attacker-controlled input exhausts SecPcreMatchLimit, rules that rely on MSC_PCRE_LIMITS_EXCEEDED or its TX compatibility indicator do not run, so a request that should be rejected can pass through the WAF. The issue affects PCRE2 deployments that use @rxGlobal with a limit-exhaustible expression and a compensating rule; it is not a universal WAF bypass. This issue is fixed in version 3.0.17.	5.8	More Details
CVE-2026-17231	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote attacker to obtain sensitive information due to an observable response discrepancy.	5.8	More Details
CVE-2026-124029	Kopia through 0.23.1 contains a path traversal vulnerability in copyDirectoryContent that allows users with repository write access to escape the restore directory via crafted entry names. Attackers can create snapshots whose directory manifest entries are named '..', so victims restoring with default options write attacker-chosen content outside the restore directory.	5.7	More Details
CVE-2026-120530	The WebToffee WP Backup and Migration plugin for WordPress is vulnerable to generic SQL Injection via the 'description' parameter in all versions up to, and including, 1.6.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. Successful exploitation requires an administrator to subsequently perform the plugin's ordinary local database export and restore operation on the same site, which is this plugin's primary intended function. Successful exploitation additionally requires an action by an administrator — the attacker cannot trigger the vulnerability on their own.	5.7	More Details
CVE-2026-85036	The Bluetooth Classic AVDTP layer defers releasing a session's stream endpoints: bt_avdtp_l2cap_disconnected() in subsys/bluetooth/host/classic/avdtp.c ends with k_work_submit(&session->_release_work), placing the embedded struct k_work on the system work queue's pending list. When the same struct bt_avdtp object is immediately reused for a new signalling connection, the session memory is re-initialized — a2dp_get_connection() in subsys/bluetooth/host/classic/a2dp.c memset()s the whole struct bt_a2dp, and bt_avdtp_l2cap_accept() / bt_avdtp_connect() call k_work_init() on session->_release_work — while that work item is still linked into k_sys_work_q.pending. Zeroing a linked sys_snode_t truncates the list while its tail pointer keeps pointing past the truncation. The reuse window is deterministic rather than a race. All host RX processing runs on the Bluetooth RX work queue at a cooperative priority (CONFIG_BT_RX_PRIO), while _release_work is submitted to the lower-priority system work queue, so the release handler cannot run until the RX thread blocks. Because l2cap_br_recv() processes every signalling command contained in a single L2CAP signalling PDU back-to-back, a peer can send one PDU holding an L2CAP Disconnection Request for the AVDTP signalling channel followed by a Connection Request for PSM 0x0019; the second command reaches the session-reuse path with the release work provably still queued. The peer must already hold an encrypted AVDTP signalling channel, i.e. be a paired/bonded BR/EDR device. The result is corruption of the global system work queue's pending list: either the queue silently stops executing any work at all (subsequent submissions are appended to a chain the head can no longer reach, and the orphaned items keep their K_WORK_QUEUED flag forever) or, in the tail variant, the list acquires a self-referencing node that the queue thread spins on. The written values are pointers to other struct k_work objects and are not attacker-controlled, so the impact is a device-wide, reboot-required denial of service rather than a controllable write primitive. Only builds with CONFIG_BT_CLASSIC and CONFIG_BT_A2DP are affected. The fix is a two-commit unit, and neither commit closes the path on its own. ec822ceed83b adds a pending-release check to bt_avdtp_connect() and bt_avdtp_l2cap_accept(), but the A2DP upper layer's a2dp_get_connection() memset()s the session — including the queued work item's list node and flags — before those checks run, so k_work_busy_get() would observe an already-cleared state. 2bd5ea88c69b closes that by making a2dp_get_connection() itself skip the reuse and return NULL while the release work is still pending, which both callers already handle by rejecting the connection attempt. Apply both commits together; either one alone leaves the device vulnerable.	5.7	More Details
CVE-2026-118239	The AutomatorWP WordPress plugin before 6.0.7 does not check that the user completing its Zoom and AWeber integration connections is allowed to do so, allowing unauthenticated attackers to replace the stored integration credentials with their own and divert the data the site sends to those services into an account they control. Exploitation requires the integration to already be connected and knowledge of the site's OAuth client identifier.	5.6	More Details
CVE-2026-121746	Node Version Manager (nvm) is a POSIX-compliant shell function for managing multiple node.js versions. In versions 0.40.0 through 0.40.8, `nvm use --save` and `nvm install --save` (or `-w`) write the resolved version to `$PWD/.nvmrc` with `tee`, which follows a symbolic link. A repository that commits `.nvmrc` as a symlink to a path outside itself (git recreates the link on clone) therefore makes `--save` truncate any file the user can write, such as a shell startup file or `~/.ssh/authorized_keys`, and replace its contents with the version string, or create the target of a dangling link; the link itself is left unchanged, so `git status` stays clean. The attacker does not control the content written, so this is data loss, not code execution. Version 0.41.0 refuses, with a warning, to write when `.nvmrc` in the current directory is a symlink, dangling or not, rather than writing through it or replacing it.	5.5	More Details
CVE-2026-17305	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to server-side request forgery.	5.5	More Details

CVE-2026-123854	In JetBrains PyCharm before 2026.3 code execution was possible in Safe Mode via a crafted Jupyter notebook widget module	5.5	More Details
CVE-2026-90627	The flat file database driver in Apache Openoffice versions through 4.1.16 allows a crafted document to read the contents of any local file without asking the user. Users are recommended to upgrade to version 4.1.17, which fixes this issue.	5.5	More Details
CVE-2026-122330	Blosc c-blosc2 before 3.5.0 contains a divide-by-zero vulnerability in blosc2_schunk_get_slice_buffer() in blosc/schunk.c that allows attackers to crash applications by supplying crafted frames with unchecked zero chunksize or blocksize values. Attackers can provide a malicious Blosc2 frame opened via blosc2_schunk_open() or blosc2_schunk_from_buffer() and read as a slice, raising SIGFPE and terminating the process.	5.5	More Details
CVE-2026-123036	A flaw was found in ansible-core. When a task marked `no_log: true` fails, the task result is censored before being emitted, but the `exception` field is retained because it is present in the PRESERVE allow-list in lib/ansible/_internal/_task.py, and the default stdout callback prints it through CallbackBase._handle_exception. As a result, sensitive values the operator explicitly asked to hide can be disclosed: module argument-validation errors echo the argument value, templating errors print an Origin source snippet (the failing line plus the two preceding lines of the variables file, exposing neighbouring secrets from an -e @secrets.yml file), and fail/assert messages are printed in full. Secret material supplied as extra variables or variables files can therefore leak to terminal output, CI logs, and the stdout logs of any automation wrapping ansible-playbook, even though every task touching the secrets is marked no_log: true. This is a regression introduced with the ansible-core 2.19 data-tagging/templating rework; the behaviour does not occur on 2.16, where the error text is correctly censored.	5.5	More Details
CVE-2026-112335	Wazuh agent from 1.0.0 before 4.14.9 contains a stack-based buffer overflow in the logcollector snort-full log reader that miscalculates remaining buffer space in read_snortfull(). Attackers who write crafted multi-line content to a monitored snort-full log can overflow the 65,280-byte stack buffer, crashing the agent or overwriting an SEH handler on 32-bit Windows agents running as SYSTEM.	5.5	More Details
CVE-2026-115426	The WPvivid — Backup, Migration & Staging WordPress plugin before 0.9.138 does not properly validate a backup storage directory path before using it to create directories and write files, allowing administrators to cause those directories and files to be created outside the intended backup location via path traversal.	5.5	More Details
CVE-2026-123316	In JetBrains Junie CLI before 26.6.29 sensitive environment variables were exposed in session event logs	5.5	More Details
CVE-2026-17067	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to access internal network resources due to server-side request forgery.	5.5	More Details
CVE-2026-123976	EDFbrowser before 2.16 contains an out-of-bounds write vulnerability in check_edf_file() that allows attackers to overflow the 256-element annot_ch array by supplying excessive annotation signals. Attackers can craft an EDF+ or BDF+ file with more than 256 annotation signals to overwrite edfhdrblock members, including the signal parameter pointer, crashing the application when opened.	5.5	More Details
CVE-2026-107129	Joomla Extension - balbooa.com - Unauthenticated arbitrary file deletion via path traversal in Gridbox < 2.20.5.0	5.5	More Details
CVE-2026-124030	GPAC through 26.07.0 contains a type confusion vulnerability in gf_sg_command_apply() in src/scenegraph/commands.c that fails to verify BIFS field-replace command types match target node fields. Attackers can supply a crafted XMT file opened with MP4Box, such as via chapter import, causing gf_sg_vrml_field_clone() to memcpy from invalid pointers and crash.	5.5	More Details
CVE-2026-48175	Processing a malformed RRC message leads to an out-of-bounds read, resulting in a denial-of-service condition.	5.5	More Details
CVE-2026-115242	The WPvivid — Backup, Migration & Staging WordPress plugin before 0.9.137 does not sanitize the staging destination folder supplied to its staging-start handler, applying only a generic text filter while the sibling writability-check handler applies the correct filename sanitizer, so an authenticated administrator can supply a path containing traversal sequences and make the WPvivid — Backup, Migration & Staging WordPress plugin before 0.9.137 write the copied site files outside the WordPress installation directory.	5.5	More Details
CVE-2026-123199	eBook-speaker 6.1.0 through 6.2.0 contains a stack buffer overflow vulnerability in get_attributes() in src/common.c caused by an unbounded strcpy of an element's name attribute. Attackers can craft an EPUB or DAISY book with a name attribute of 511 or more characters to corrupt the stack and crash the reader when opened.	5.5	More Details
CVE-	Node Version Manager (nvm) is a POSIX-compliant shell function for managing multiple node.js versions. In versions 0.2.0 through 0.40.8, nvm does not check whether `.nvmrc` is a symbolic link. A repository or archive that ships `.nvmrc` as a symlink to another file (for example `../../.npmrc`, or `/proc/self/environ` on Linux) makes a plain `nvm use`, `nvm install`, `nvm which`, `nvm exec`, `nvm run`, or `nvm-exec` read that file and print its contents in the invalid-`.nvmrc` message (even with `--silent`) or, for a one-line file, in the `Found ... with version		More

2026-121747	<...>` message; with the README's zsh `load-nvmrc` or bash `cdnvm` hook installed, entering the directory is enough. nvm sends the content nowhere; the attacker learns it only where they can see the victim's output, such as a CI log for a contributed branch. Version 0.41.0 still follows a symlinked `.nvmrc`, so deliberate links to another version file keep working, but never prints its content, and accepts it only if it contains a version or the name of an existing alias; the README's bash `cdnvm` hook, which read `.nvmrc` itself, now gets the version from nvm, so users of that hook must also update their copy of it.	5.5	Details
CVE-2026-124031	GPAC through 26.07.0 contains a type confusion vulnerability in drawable_get_aspect_2d_mpeg4() and TraverseShape() that casts a Shape's appearance node to M_Appearance without checking its node tag. Attackers can supply a crafted XMT file placing another node type, such as Conditional, in the appearance field to trigger an invalid memory read and crash MP4Box.	5.5	More Details
CVE-2026-121944	sngrep through 1.9.0 contains an infinite loop vulnerability in capture_packet_reasm_ip() in src/capture.c that allows attackers to cause denial of service via crafted NFLOG TLVs. Attackers can supply a pcap file with link type NFLOG containing a non-payload TLV with length under 4, making the capture thread spin at full CPU and stop processing packets.	5.5	More Details
CVE-2026-46429	GeoNode is a geospatial content management system, a platform for the management and publication of geospatial data. Prior to 5.0.3, specially crafted requests can circumvent GeoNode upload service validation, allowing a low-privileged remote user to store and serve malicious files. This issue is fixed in version 5.0.3.	5.5	More Details
CVE-2025-54991	JupyterLab Desktop is the cross-platform desktop application for JupyterLab. Prior to 4.6.2-1, JupyterLab Desktop for macOS declared the com.apple.security.cs.allow-dyld-environment-variables entitlement, allowing the dynamic linker to honor DYLD_INSERT_LIBRARIES despite the hardened runtime. An attacker who can already execute code as the current user can load an arbitrary dynamic library into the JupyterLab Desktop process and inherit TCC permissions previously granted to the application, including access to protected Documents, Desktop, or Downloads folders without another macOS prompt. Exploitation requires existing local code execution and prior TCC grants; it does not provide initial or remote code execution. Windows and Linux are not affected. This vulnerability is fixed in 4.6.2-1.	5.5	More Details
CVE-2025-55002	JupyterLab Desktop is the cross-platform desktop application for JupyterLab. Prior to 4.6.2-1, JupyterLab Desktop for macOS shipped with Electron's RunAsNode fuse enabled, allowing ELECTRON_RUN_AS_NODE to execute arbitrary Node.js code in the application process. An attacker who can already execute code as the current user can therefore run code in JupyterLab Desktop's context and inherit TCC permissions previously granted to the application, including access to protected Documents, Desktop, or Downloads folders without another macOS prompt. Exploitation requires existing local code execution and prior TCC grants; it does not provide initial or remote code execution. Windows and Linux are not affected. This vulnerability is fixed in 4.6.2-1.	5.5	More Details
CVE-2026-90632	Apache OpenOffice documents can include multimedia content (audio, video, etc.) A crafted document could exploit the GStreamer multimedia component of Apache OpenOffice version through 4.1.16 to load the contents of any local file, and include them when the document is saved or exported, for example as PDF. Users are recommended to upgrade to version 4.1.17, which fixes this issue.	5.5	More Details
CVE-2026-59263	A manipulated document opened in Apache OpenOffice 4.1.16 or earlier may allow substituted content to be displayed manipulating the user. Such documents are corrupt and should not be opened. Users are recommended to upgrade to version 4.1.17, which fixes this issue.	5.5	More Details
CVE-2026-73473	A flaw was found in GStreamer gst-plugins-good (avidemux). In the subindex parser, missing validation of the entry count can cause excessive memory allocation and denial of service. Because avidemux is auto-plugged by playbin, decodebin, and gst-discoverer, opening or previewing a crafted AVI is sufficient to trigger the issue. Fixed upstream in gst-plugins-good 1.28.6 (GStreamer-SA-2026-0072).	5.5	More Details
CVE-2026-123785	Fluxbox through 1.3.7 contains an infinite loop vulnerability in Menu::updateMenu() in src/FbTk/Menu.cc that allows attackers to hang the window manager via crafted style geometry values. Attackers can supply a style with an oversized unbounded menu.titleHeight so the column loop never terminates, causing sustained CPU use and denial of service at startup.	5.5	More Details
CVE-2026-109837	Authorization Bypass Through User-Controlled Key in Order Returns in Apache OFBiz 24.09 before 24.09.08 on all platforms allows an authenticated user with low-privileged Order Manager access to associate another party's OrderItem with a ReturnItem on a ReturnHeader they control, via the createReturnItem service. Users are recommended to upgrade to version 24.09.08, which fixes this issue.	5.4	More Details
CVE-2026-123664	A security flaw has been discovered in nasa-gcn gcn.nasa.gov up to b299b562af665878964b981a459f0a9c04b11adf. This issue affects some unknown processing of the file /user/email of the component Email Notification Handler. Performing a manipulation of the argument Recipient results in improper authorization. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks. This product adopts a rolling release strategy to maintain continuous delivery. Therefore, version details for affected or updated releases cannot be specified. The pull request to fix this issue awaits acceptance.	5.4	More Details
CVE-2026-123624	ChatWiki before 2.10.0 contains an insecure direct object reference vulnerability that allows authenticated users to modify other tenants' fast commands by supplying arbitrary sequential ids to POST /manage/saveFastCommand. Attackers can overwrite another tenant's command title, type, content and robot binding, redirecting webpage-jump commands to attacker URLs and reassigning the record to their own tenant.	5.4	More Details

CVE-2026-109129	Authorization Bypass Through User-Controlled Key in the Order Manager component in Apache OFBiz 24.09.07 on all platforms allows an authenticated user with only view-level order permissions to modify or create OrderPaymentPreference records belonging to orders outside their authorized scope via the updateOrderPaymentPreference service, by supplying an orderPaymentPreferenceId belonging to a different order. Users are recommended to upgrade to version 24.09.08, which fixes this issue.	5.4	More Details
CVE-2026-54380	VitaFit cloud API before 2026-10-30 contained a stored cross-site scripting vulnerability that allows authenticated attackers to upload an SVG image containing malicious JavaScript to the shared storage bucket. Attackers can exploit the application's failure to restrict scripts or force downloads for image/svg+xml content, causing the JavaScript to execute when a victim opens the file via direct browser navigation.	5.4	More Details
CVE-2026-103863	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Apache Sling Engine. Content-Type, charset, and redirect changes from an included component evade the protectheaders / checkcontenttype enforcement through setHeader(), repeated calls to setContentType(), the charset APIs, Servlet 6.1 redirect overloads, and stale config - enabling stored XSS despite enabled protections. This issue affects Apache Sling Engine before 3.0.4. Users are recommended to upgrade to version 3.0.4, which fixes the issue.	5.4	More Details
CVE-2026-17114	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information and cause a denial of service due to the generation of error messages containing sensitive information.	5.4	More Details
CVE-2026-17369	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote attacker to force a user to authenticate into an attacker-controlled account due to cross-site request forgery. The sign-in flow does not sufficiently verify that a login response belongs to the user's own request, which could link the victim's session to an account controlled by the attacker.	5.4	More Details
CVE-2026-17139	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to execute arbitrary scripts due to cross-site scripting. Certain URL fields are not sufficiently validated, so malicious script content could run in another user's browser session.	5.4	More Details
CVE-2026-121766	Missing Authorization vulnerability in Blubrry Podcasting PowerPress Podcasting powerpress allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects PowerPress Podcasting: from n/a through 11.18.0.	5.4	More Details
CVE-2026-12550	IBM MQ 9.2.0.0 through 9.2.0.44 LTS, 9.3.0.0 through 9.3.0.42 LTS, 9.4.0.0 through 9.4.0.26 LTS, 9.4.0.0 through 9.4.5.1 CD, and 10.0.0.0 through 10.0.0.5 LTS and CD could allow an authenticated attacker to obtain sensitive information or cause a denial of service due to improper validation of message selection parameters.	5.4	More Details
CVE-2026-17367	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to insufficiently protected credentials.	5.4	More Details
CVE-2026-120035	The RSS Aggregator by Feedzy – Feed to Post, Autoblogging, News & YouTube Video Feeds Aggregator plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'item_title (parsed from feed <item><title>)' parameter in all versions up to, and including, 5.2.13 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This requires an administrator to have previously configured a Feed-to-Post import pointing at an attacker-controlled feed URL, after which the attacker can rotate payloads at will without any further interaction with the site.	5.4	More Details
CVE-2026-123329	In JetBrains YouTrack before 2026.2.19562 missing authorization in TeamCity integration allowed disclosure of other projects' actions	5.4	More Details
CVE-2026-103908	The The AMP for WP – Accelerated Mobile Pages plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 1.1.18. 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 custom-level access and above, to execute arbitrary shortcodes. The vulnerable output block is gated by the 'ampforwp-cat-description' setting, which is enabled by default, meaning the vast majority of installations are affected without any additional configuration change.	5.4	More Details
CVE-2026-118407	The Premium Packages WordPress plugin before 7.3.1 does not verify that a user claiming a guest order is the original buyer, allowing any authenticated user to take ownership of any unclaimed guest order, and thereby read the buyer's billing details and download their purchased files, by supplying only the order identifier.	5.4	More Details
CVE-2026-17230	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to a path traversal vulnerability.	5.4	More Details
CVE-2026-107658	The BuddyForms plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'bf_post_type (and buddyforms_form_content)' parameter in all versions up to, and including, 2.10.5 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Exploitation requires that at least one BuddyForms form with public submissions enabled exists on the site (so that the required nonce can be	5.4	More Details

	harvested from the public form page) and that the active theme registers a widgetized sidebar, allowing the injected customize_changeset to place a malicious Custom HTML widget into the site's front end.		
CVE-2026-17225	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to bypass security restrictions and access unauthorized analytics queries due to improper input validation. Request parameters are not validated sufficiently, which could allow restrictions on analytics data to be circumvented.	5.4	More Details
CVE-2026-119178	The Smart Cookie Kit plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'comment' parameter in all versions up to, and including, 2.3.2 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 payload is specifically crafted to survive wp_kses on save by storing hostile characters inside allowed HTML elements, with the attribute-breaking double-quote smuggled inside a permitted <code> body and reconstructed into a <abbr title> attribute only at render time by the plugin's own output buffer; exploitation requires an administrator to approve the comment and subsequently view the affected public post.	5.4	More Details
CVE-2026-17312	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote attacker to force a user to authenticate into an attacker-controlled account due to cross-site request forgery. The sign-in flow does not sufficiently verify that a login response belongs to the user's own request, which could link the victim's session to an account controlled by the attacker.	5.4	More Details
CVE-2026-123310	In JetBrains IntelliJ IDEA before 2026.3 kotlin scripts could trigger dependency downloads from arbitrary repositories in untrusted projects	5.4	More Details
CVE-2026-35110	HCL AION is affected by a vulnerability where encrypted (HTTPS) communication was not enforced for all requests. Data may be transmitted over unencrypted connections and intercepted by an attacker on the network, potentially resulting in unintended behavior or security impact under certain conditions.	5.4	More Details
CVE-2026-118067	The Form Maker by 10Web – Mobile-Friendly Drag & Drop Contact Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'wdform_<field_id>_element<form_id> (payload) + disabled_fields<form_id> (pivot)' parameter in all versions up to, and including, 1.15.50 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 targeted form to contain a File Upload field, as the attacker must suppress that field's storage row via the disabled_fields parameter to shift a controlled text-field value into the positional slot where escaping is skipped; execution occurs when an administrator opens the Submissions page for the affected form.	5.4	More Details
CVE-2026-120514	The Zephyr Project Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'zpm_profile_picture' parameter in all versions up to, and including, 3.3.209 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 injected payload is stored in the subscriber's own Zephyr profile and fires in any Administrator's browser session the first time the autocomplete mention lookup renders the avatar field, requiring no additional configuration beyond the plugin's default access_roles setting. Successful exploitation additionally requires an action by an administrator — the attacker cannot trigger the vulnerability on their own.	5.4	More Details
CVE-2026-17154	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to perform cross-site scripting due to improper neutralization of user-supplied input.	5.4	More Details
CVE-2026-88982	Kubeflow Pipelines enables users to build and deploy portable, scalable machine learning workflows. Prior to 2.18.0, the legacy V1/raw-Argo execution cache mutating webhook and cache-server storage path hash selected template fields without the Kubernetes namespace, use the key alone for lookups and duplicate checks, and trust the mutable pipelines.kubeflow.org/execution_cache_key annotation when publishing outputs. In multi-user deployments where tenant namespaces share the cache service, a tenant with workload-submission privileges can read another namespace's cached outputs or seed matching outputs that are substituted into a later step. Standard KFP V2 component pods bypass this cache, matching requires the selected template fields and staleness policy, and arbitrary code execution or service availability impact is not established. This issue is fixed in version 2.18.0.	5.4	More Details
CVE-2026-96460	A flaw was found in the token exchange mechanism of Keycloak. When using Standard Token Exchange V2, the system issues new tokens with a fresh lifetime based on the requester clients configuration instead of limiting it to the original tokens expiration. This issue allows an authenticated requester to indefinitely extend access for service accounts by repeatedly exchanging tokens, even if the original client has been disabled by an administrator.	5.4	More Details
CVE-2026-122659	Missing Authorization vulnerability in WP ManageNinja LLC Fluent Booking fluent-booking allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Fluent Booking: from n/a through 2.5.0.	5.4	More Details
CVE-2026-	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to execute arbitrary	5.4	More

17155	scripts due to improper neutralization of user-controlled input.		Details
CVE-2026-123331	In JetBrains YouTrack before 2026.2.19197 article editors could change visibility of restricted child articles	5.4	More Details
CVE-2026-122670	Missing Authorization vulnerability in WP SYNTEX Polylang polylang allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Polylang: from n/a through 3.9.	5.4	More Details
CVE-2026-123289	In JetBrains Datalore before 2026.4 improper authorisation allowed notebook viewers to modify files	5.4	More Details
CVE-2026-100360	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to 7.15.2 and 8.10.2, V8 API relationship write paths do not consistently enforce object-level edit and view authorization on both related records. In the verified Account-to-Contact case, an authenticated user can create a relationship while unable to edit the Account and can delete relationship links to a hidden Contact that cannot be viewed directly. This issue is fixed in versions 7.15.2 and 8.10.2.	5.4	More Details
CVE-2026-123851	In JetBrains Junie GitHub Action before 1.6.4 prompt injection protection could be bypassed via HTML-encoded characters	5.4	More Details
CVE-2026-76580	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in OpenText OpenText Directory Services (OTDS) on Windows and Linux allows Cross-Site Scripting (XSS). This issue affects OpenText Directory Services (OTDS): from 25.1 through 26.2.	5.4	More Details
CVE-2026-108588	IBM Db2 Genius Hub 1.1.2, 1.1.3, 1.1.4, 1.1.5 could allow a remote authenticated attacker to bypass security restrictions due to a missing X-Content-Type-Options header allowing MIME type sniffing.	5.4	More Details
CVE-2026-120683	The Real Testimonials – Testimonial Slider, Collect Customer Reviews and Video Testimonials plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'tpro_client_testimonial' parameter in all versions up to, and including, 4.1.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Successful exploitation requires an administrator to approve the pending testimonial through standard moderation and the target page to load the WordPress Interactivity runtime (e.g. a theme or block that enqueues @wordpress/interactivity).	5.4	More Details
CVE-2026-1339	An Open Redirect vulnerability has been identified in OpenText™ Universal Discovery and CMDB. The vulnerability can be exploited only if an attacker sends a specially crafted URL containing a link to a malicious resource and a user subsequently follows that link. Affected systems: This issue affects only the classic deployment options for UCMDB UI (ucmdb-browser) component within Universal Discovery and CMDB and Operations Bridge Manager. Containerized deployment options are not affected.	5.4	More Details
CVE-2026-121008	SQL::Abstract::Tree versions before 2.000001_04 for Perl allow cross-site scripting via unescaped SQL text and bind values in the html profile. The html profile wraps keywords and placeholders in span elements and breaks lines with br elements, so its output is meant to go into a page as is. The format method does not HTML-escape the SQL text or the bind values it fills in around that markup. An application that renders SQL formatted with the html profile, such as in a debug panel or query log, allows an attacker who controls a bind value or part of the SQL text to embed JavaScript in the page.	5.4	More Details
CVE-2026-119467	Missing Authorization vulnerability in WPVibes AnyWhere Elementor anywhere-elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects AnyWhere Elementor: from n/a through 1.3.0.	5.4	More Details
CVE-2026-120685	The Real Testimonials – Testimonial Slider, Collect Customer Reviews and Video Testimonials plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'tpro_client_image (JPEG IPTC caption) + tpro_client_testimonial ([gallery] shortcode)' parameter in all versions up to, and including, 4.1.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This requires an administrator to have the display block configured with the Strip All HTML Tags option disabled, which is the plugin's native setting for rendering formatted testimonial content, and to have approved the submitted testimonials.	5.4	More Details
CVE-2026-85744	FreeScout is a self-hosted help desk and shared mailbox. Prior to 1.8.227, the conversation_merge action records a failed authorization check for the target conversation in response['msg'] and then clears that value inside the source-conversation loop. An authenticated agent can merge a conversation they control into a target conversation in a mailbox they cannot access. The operation injects threads, attachments, and audit records into the unauthorized target and deletes the source conversation, but it does not disclose the target's existing contents. This issue is fixed in version 1.8.227.	5.4	More Details
CVE-	HomeBox is a home inventory and organization system. Prior to 0.27.0, the maybeUrl() utility accepts markdown-style links in entity custom-field values without restricting the URL scheme, so an authenticated user can store a		

2026-75599	javascript: URI that is rendered as a clickable anchor on an item page. When another authenticated user clicks the link, attacker-controlled JavaScript executes in the victim's HomeBox origin, enabling session theft, account takeover, or data exfiltration. This issue is fixed in version 0.27.0.	5.4	More Details
CVE-2026-52713	Missing Authorization vulnerability in ThimPress LearnPress learnpress allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects LearnPress: from n/a through 4.4.12.	5.4	More Details
CVE-2026-94618	FileGator is a multi-user file manager. Prior to 7.15.0, GET /batchdownload in backend/Controllers/DownloadController.php uses batchDownloadStart() to stream a shared temporary archive selected by the request-supplied uniqid without checking that the current session created it. In deployments with distinct per-user home directories, a valid user with read, download, and batchdownload permissions who obtains another user's active archive id can cross that boundary and retrieve the victim's batch archive. The archive lifetime and id-acquisition requirement limit exploitation, but a successful replay also deletes the victim's pending archive. This issue is fixed in version 7.15.0.	5.4	More Details
CVE-2026-122675	Cross-Site Request Forgery (CSRF) vulnerability in Wpmet Wp Social wp-social allows Cross Site Request Forgery.This issue affects Wp Social: from n/a through 3.2.3.	5.4	More Details
CVE-2026-121949	The Symfony HtmlSanitizer component does not apply the media URL policy to the srcset and imagesrcset attributes, allowing values that point to hosts or schemes not permitted by allowMediaSchemes() or allowMediaHosts() to bypass it, so that browsers load images from disallowed hosts in Symfony versions 6.1.x prior to 6.4.50, 7.x prior to 7.4.23, and 8.x prior to 8.1.11.The srcset attribute on img and source elements and the imagesrcset attribute on link elements are allowed by the sanitizer, but their URL candidates are never validated, so their values are kept verbatim while the same URL in src is dropped. The fixes for CVE-2026-45753 and CVE-2026-48761 extended the same attribute list but did not cover these two attributes. For example, with allowMediaSchemes(['https']) and allowMediaHosts(['trusted.example']), <img srcset="https://evil.example/a.png 1x"> survives sanitization, and the browser fetches the selected candidate as it would fetch src. Candidates with a scheme forbidden by the configuration, such as http, are kept as well. Any application that sanitizes untrusted HTML and relies on the media schemes and hosts allowlists to restrict where images can be loaded from is affected. A single crafted value is enough to make the browser of a user viewing the sanitized content send a request to an attacker-controlled host, which can be used to track viewers or log their IP addresses. No authentication is needed if the application accepts HTML from unauthenticated users.	5.4	More Details
CVE-2026-121515	The FV Flowplayer Video Player plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'comment' parameter in all versions up to, and including, 7.5.56.7212 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This requires the 'Parse Vimeo and YouTube links' option to be enabled, and the injected comment must be approved before the script executes for site visitors.	5.4	More Details
CVE-2026-123288	In JetBrains Datalore before 2026.4 stored XSS in notebook charts was possible via Vega editor link	5.4	More Details
CVE-2026-120741	The MotoPress Appointment Booking Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to, and including, 2.4.8 via the public '/motopress/appointment/v1/customers/create' REST endpoint. The route is registered with permission_callback => '__return_true' and the handler's 'name' parameter is not sanitized before being written to the custom wp_mpa_customers table via $wpdb->insert, nor is it escaped on output in the admin bookings list when the viewing user lacks the 'mpa_edit_customer' capability (such as the plugin-defined Appointment Employee role). This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.4	More Details
CVE-2026-106136	Cross-Site Scripting (XSS) in the Chat component (@progress/kendo-react-conversational-ui) in Progress Software KendoReact versions 0.6.0 through 16.1.0 allows a low-privileged attacker who can supply Chat messages to execute arbitrary JavaScript in the origin of the application via an unsafe URL in an openUrl quick action, which runs when a user clicks the action.	5.4	More Details
CVE-2026-119152	The Appointment Booking Plugin – LatePoint | Calendar & Scheduling for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'customer[email] (inside params)' parameter in all versions up to, and including, 5.7.6 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. An unauthenticated visitor can exploit this by registering as a LatePoint customer via the public booking form — receiving an active customer session with no WordPress account — and then submitting a quoted local-part email address containing an HTML payload (e.g. a tag with no spaces) that passes FILTER_VALIDATE_EMAIL but is stored and rendered unescaped.	5.4	More Details
CVE-2026-84728	Incorrect Authorization in Apache OFBiz 24.09 before 24.09.08 on all platforms, when documented multitenancy is enabled, allows a remote authenticated attacker holding only a valid low-privilege account in one tenant to read and write data belonging to a different tenant, by submitting their own tenant's userTenantId alongside their own credentials to the normal Party Manager login against a hostname mapped to a different tenant: ContextFilter resolves the tenant from the hostname via TenantDomainName, but LoginWorker gives priority to the conflicting userTenantId request parameter and authenticates against the attacker's own tenant, so a	5.4	More Details

	subsequent ordinary request to the same hostname combines the hostname-mapped tenant's Entity Engine delegator with the attacker's tenant's session dispatcher, security object, and identity, letting the permission check run against the attacker's own tenant while the resulting read or write is performed against the hostname-mapped tenant's data. Users are recommended to upgrade to version 24.09.08, which fixes this issue.		
CVE-2026-123330	In JetBrains YouTrack before 2026.2.19562 missing authorization allowed users with read-only access to change issue visibility settings	5.4	More Details
CVE-2026-12538	IBM MQ 9.4.0.0 to 9.4.0.26, 9.4.1.0 to 9.4.5.3, and 10.0.0.1 to 10.0.0.5 could allow an authenticated attacker to obtain sensitive information or cause a denial of service due to improper validation of message header structure length fields.	5.4	More Details
CVE-2026-119218	The Greenshift – animation and page builder blocks plugin for WordPress is vulnerable to Stored DOM-Based Cross-Site Scripting via the 'url (comment_author_url)' parameter in all versions up to, and including, 13.2.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Exploitation requires the affected page to be configured with a GreenShift Interaction Layer attach-attribute action that copies a comment-author anchor's href into a Counter block's data-prefix or data-postfix attribute; given that configuration, the payload executes for every visitor who loads the Counter into the viewport once the comment is published.	5.4	More Details
CVE-2026-106134	Cross-Site Scripting (XSS) in the Menu component (@progress/kendo-react-layout) in Progress Software KendoReact versions 1.3.0 through 16.1.0 allows a low-privileged attacker who can influence the Menu item data to execute arbitrary JavaScript in the origin of the application via an unsafe URL in a Menu item, which runs when a user selects the item.	5.4	More Details
CVE-2026-119219	The Jupiter X Core plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'fields[<custom_meta_field_id>]' parameter in all versions up to, and including, 4.62.0 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. Execution requires that the attacker-registered account be assigned as the post_author of a page or post whose template includes the Raven Author Box widget, a fixture an administrator can create by reassigning authorship to any user including newly registered Subscribers.	5.4	More Details
CVE-2026-103939	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to 8.3.0, interface/modules/custom_modules/oe-module-weno/scripts/file_download.php has no ACL or CSRF check and ignores the result of validateAdminCredentials(). When the Weno module is enabled, the default GET path calls PharmacyService::removeWenoPharmacies() before attempting a refetch, allowing any authenticated user to truncate the weno_pharmacy table and allowing a cross-site request to trigger the same operation through a logged-in victim. A failed later download can leave the e-prescribing pharmacy directory empty and unavailable. This issue is fixed in version 8.3.0.	5.4	More Details
CVE-2026-106135	Cross-Site Scripting (XSS) in the Chat component (@progress/kendo-angular-conversational-ui) in Progress Software Kendo UI for Angular versions prior to 25.3.0 allows a low-privileged attacker who can supply Chat messages to execute arbitrary JavaScript in another user's browser via an unsafe URL in an openUrl quick action, which runs when the user clicks the action.	5.4	More Details
CVE-2026-106141	Cross-Site Scripting (XSS) in the Editor component (@progress/kendo-angular-editor) in Progress Software Kendo UI for Angular versions prior to 25.3.0 allows a low-privileged attacker who can supply Editor content to execute arbitrary JavaScript in another user's browser via a link or image with an unsafe URL in the Editor content, which runs when the user interacts with it.	5.4	More Details
CVE-2026-106142	Cross-Site Scripting (XSS) in the Editor component (@progress/kendo-react-editor) in Progress Software KendoReact versions 2.7.0 through 16.1.0 allows a low-privileged attacker who can supply Editor content to execute arbitrary JavaScript in another user's browser via a link with an unsafe URL in the Editor content, which runs when the user clicks the link.	5.4	More Details
CVE-2026-106143	Cross-Site Scripting (XSS) in the Editor component (@progress/kendo-vue-editor) in Progress Software Kendo UI for Vue versions 2.7.1 through 10.0.0 allows a low-privileged attacker who can supply Editor content to execute arbitrary JavaScript in another user's browser via an unsafe URL entered in the Insert Link or Insert Image dialog, which runs when the user clicks the resulting link.	5.4	More Details
CVE-2026-106715	NewsBreak for Android version 26.21.0 treats data:text/html; URLs as trusted in its WebView JavaScript bridge origin check. An attacker can supply such a page through the newsbreak://openweb deep link and invoke NBJS.callNative with the getLoginInfo action, disclosing a signed-in user's account information and session token after the user opens the crafted link.	5.4	More Details
CVE-2026-121977	The JetFormBuilder — Dynamic Blocks Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'note (form field whose value is written to post meta `note`)' parameter in all versions up to, and including, 3.6.8 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. Successful exploitation requires a privileged user with the edit_others_posts capability to visit a form URL containing the attacker-created post ID, a delivery step the attacker controls via a crafted phishing link.	5.4	More Details

CVE-2026-123094	Huginn before 2026.11.05 contains a stored cross-site scripting vulnerability in the service_label helper that marks unescaped OAuth service display names as html_safe. Authenticated attackers can connect an OAuth account with a crafted nickname, name or email and share it globally, executing JavaScript when victims attach it to Agents and view them, exposing Credentials, Agents and Events, and admin actions if the victim is an administrator.	5.4	More Details
CVE-2026-90963	The Essential Real Estate WordPress plugin before 5.3.5 does not perform any authorization or publication-status check in one of its AJAX actions, allowing unauthenticated users to read the full contents of property listings that have not been published, together with the private name, email address, phone number and office address of the listing agent.	5.3	More Details
CVE-2026-120659	The Redirection for Contact Form 7 plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 3.2.14 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 write arbitrary post meta values to newly created lead posts and copy arbitrary server-side files with allowed MIME-type extensions into the plugin's uploads directory. Exploitation requires a published Contact Form 7 form configured with the Save Entry (Save Lead) action enabled on the target site.	5.3	More Details
CVE-2026-93370	The Paystack WooCommerce Payment Gateway plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 5.8.5 via the 'key' parameter. This makes it possible for unauthenticated attackers to extract customer PII — including billing name, email address, phone number, billing address, shipping address, and purchased product list — embedded into page HTML via wp_localize_script by enumerating sequential order IDs. This is only exploitable when the merchant has enabled the optional custom metadata feature in the Paystack gateway settings.	5.3	More Details
CVE-2026-103020	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to 8.3.0, the webroot admin.php multisite administration page is enabled without an authentication check, reads database configuration from sqlconf.php, and connects to each configured site database. An unauthenticated network actor can obtain site identifiers, database names, site names, exact OpenEMR versions and patch levels, pending upgrade status, and direct login and patient-portal links. This issue is fixed in version 8.3.0.	5.3	More Details
CVE-2026-121767	Missing Authorization vulnerability in weDevs weDocs wedocs allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects weDocs: from n/a through 2.6.1.	5.3	More Details
CVE-2026-121778	Missing Authorization vulnerability in WP Lab WP-Lister Lite for Amazon wp-lister-for-amazon allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP-Lister Lite for Amazon: from n/a through 2.9.2.	5.3	More Details
CVE-2026-119498	Authentication Bypass Using an Alternate Path or Channel vulnerability in RelyWP Simple Cloudflare Turnstile simple-cloudflare-turnstile allows Authentication Abuse.This issue affects Simple Cloudflare Turnstile: from n/a through 1.44.4.	5.3	More Details
CVE-2026-90965	The Essential Real Estate WordPress plugin before 5.3.5 does not perform a publication-status or authorization check in two of its AJAX actions, allowing unauthenticated users to retrieve the images attached to property listings that have not been published.	5.3	More Details
CVE-2026-121779	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in YITH YITH WooCommerce Subscription yith-woocommerce-subscription allows Retrieve Embedded Sensitive Data.This issue affects YITH WooCommerce Subscription: from n/a through 4.22.0.	5.3	More Details
CVE-2026-121781	Missing Authorization vulnerability in WP ManageNinja LLC Fluent Booking fluent-booking allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Fluent Booking: from n/a through 2.5.0.	5.3	More Details
CVE-2026-119494	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Gemini Labs Site Reviews site-reviews allows Code Injection.This issue affects Site Reviews: from n/a through 8.3.6.	5.3	More Details
CVE-2026-124274	Missing Authorization vulnerability in myCred myCred mycred allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects myCred: from n/a through 4.0.2.	5.3	More Details
CVE-2026-39733	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in properfraction ProfilePress wp-user-avatar allows Code Injection.This issue affects ProfilePress: from n/a through 4.17.7.	5.3	More Details
CVE-2026-123311	In JetBrains IntelliJ IDEA before 2026.3, 2026.2.4 command execution via a hidden run control in the Markdown preview was possible	5.3	More Details
CVE-2026-73580	Missing authorization check in the getHRChild service in Apache OFBiz through 24.09.07 on all platforms allows a remote unauthenticated attacker to recursively enumerate Human Resources organization and employee data, including department names and identifiers, employment position names and identifiers, employee party identifiers, position occupancy, and organization relationships, via a crafted partyId parameter. Users are	5.3	More Details

	recommended to upgrade to version 24.09.08, which fixes this issue.		
CVE-2026-83538	Missing Authorization in Apache OFBiz 24.09 before 24.09.08 on all platforms allows a remote unauthenticated attacker to disclose internal business records — including organization, employee, product catalog, and product-store data — by requesting several helper endpoints across the Human Resources, Catalog, and Order Manager applications that are configured to skip authentication and perform no permission check before returning the requested record. Users are recommended to upgrade to version 24.09.08, which fixes this issue.	5.3	More Details
CVE-2026-119465	Insertion of Sensitive Information Into Sent Data vulnerability in WPVibes Elementor Addon Elements addon-elements-for-elementor-page-builder allows Retrieve Embedded Sensitive Data.This issue affects Elementor Addon Elements: from n/a through 1.15.	5.3	More Details
CVE-2026-123290	In JetBrains Datalore before 2026.4 hidden notebook code was exposed to unauthenticated users via the public interactive report content endpoint	5.3	More Details
CVE-2026-103021	OpenEMR is a free and open source electronic health records and medical practice management application. From 6.0.0 until 8.3.0, interface/globals.php uses the unauthenticated authUser login parameter to populate temp_authuserid and load that account's user_settings before authentication succeeds. Existing usernames can therefore cause an additional database query and may apply visible customized settings, while nonexistent usernames skip that behavior. A remote unauthenticated actor can use timing or page differences to enumerate valid accounts for later credential attacks. This issue is fixed in version 8.3.0.	5.3	More Details
CVE-2026-120842	Missing Authorization vulnerability in Brainstorm Force SureForms sureforms allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects SureForms: from n/a through 2.13.0.	5.3	More Details
CVE-2026-87856	The Subscriptions for WooCommerce WordPress plugin before 2.1.1 only enforces its membership content restrictions on standard front-end page views, allowing unauthenticated users to read the full contents of restricted posts and pages through other routes that render the same content.	5.3	More Details
CVE-2026-119496	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in David Lingren Media LIbrary Assistant media-library-assistant allows Code Injection.This issue affects Media LIbrary Assistant: from n/a through 3.43.	5.3	More Details
CVE-2026-122138	BlueprintUE Self-Hosted Edition 4.2.0 before 4.3.4 contains a login rate limit bypass vulnerability in LoginMiddleware.php that keys failed-login counters on case-sensitive usernames. Unauthenticated attackers can vary username casing against case-insensitive MySQL lookups to get extra attempts and brute-force passwords past the per-account lockout.	5.3	More Details
CVE-2026-122129	CESNET ipfixcol2 2.7.1 before 2.9.0 contains a memory allocation vulnerability in Lz4Decoder::read_start_header() that allows unauthenticated attackers to exhaust memory by declaring unbounded ring buffer sizes. Attackers can open TCP connections sending LZ4 start headers with very large buffer sizes, forcing up to 4 GiB allocations per connection and denying collector service.	5.3	More Details
CVE-2026-123844	In JetBrains IntelliJ IDEA before 2026.3 sSRF was possible via custom plugin repositories	5.3	More Details
CVE-2026-123847	In JetBrains IntelliJ IDEA before 2026.3 command execution was possible via control characters in terminal command completion	5.3	More Details
CVE-2026-62850	FreeScout is a self-hosted help desk and shared mailbox. Prior to 1.8.225, the administrative tools.php maintenance endpoint is reachable without an appropriate authentication or access-control boundary. Response differences for attacker-controlled path values disclose whether arbitrary directories and files exist on the server. The same endpoint validates application-key and database-password candidates without rate limiting, per-session throttling, or a CAPTCHA, allowing unrestricted guessing attempts against application secrets. This issue is fixed in version 1.8.225.	5.3	More Details
CVE-2025-71455	vtenext before 25.02.2 contains a session identifier disclosure vulnerability that allows attackers to read the PHPSESSID value returned by the Touch web service endpoint. Attackers who can run script in the vtenext origin, such as through cross-site scripting, can bypass the HttpOnly flag and hijack authenticated sessions.	5.3	More Details
CVE-2026-115574	Zulip is an open-source team collaboration tool. From 11.0 until 12.2, organizations with web-public channels enabled exposed the GET /json/users endpoint to logged-out spectators, and a missing access-control check allowed include_custom_profile_fields=true to return every user's custom profile field values in addition to the documented limited directory data. This exposed those custom profile field values to unauthenticated visitors. This issue is fixed in version 12.2.	5.3	More Details
CVE-2026-123861	Authorization Bypass Through User-Controlled Key vulnerability in CrocoBlock JetFormBuilder – Hierarchical Select jet-form-builder-hierarchical-select allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects JetFormBuilder – Hierarchical Select: from n/a through 1.0.10.	5.3	More Details
CVE-	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Made with Fuel		

2026-119490	Ltd. Better Notifications for WP bnfw allows Code Injection.This issue affects Better Notifications for WP: from n/a through 1.10.1.	5.3	More Details
CVE-2026-119508	Missing Authorization vulnerability in Mamunur Rashid Radius Booking — Booking Calendar for Appointments & Services radius-booking allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Radius Booking — Booking Calendar for Appointments & Services: from n/a through 1.0.20.	5.3	More Details
CVE-2026-19319	IBM Watson Speech Services Cartridge 4.0.0 through 5.4.0 could allow a remote attacker to obtain sensitive information due to an out-of-bounds read.	5.3	More Details
CVE-2026-119513	Missing Authorization 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 5.0.3.	5.3	More Details
CVE-2026-119523	Missing Authorization vulnerability in Cozmoslabs Paid Member Subscriptions paid-member-subscriptions allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Paid Member Subscriptions: from n/a through 3.1.3.	5.3	More Details
CVE-2026-20241	A vulnerability in the authorization mechanism of Cisco Identity Services Engine (ISE) and Cisco ISE Passive Identity Connector (ISE-PIC) could allow an unauthenticated, remote attacker to obtain an endpoint identity certificate. This vulnerability is due to improper authorization checks. An attacker could exploit this vulnerability by sending a crafted request to an affected device. A successful exploit could allow the attacker to bypass authorization to obtain an endpoint certificate.	5.3	More Details
CVE-2026-123988	A vulnerability has been found in SililaWijesinghe Food Ordering System up to ba314e897e3365600461e5ea59432e39ceaa0fa5. This issue affects some unknown processing of the file /Food-Ordering-System/admin/. Such manipulation leads to exposure of information through directory listing. 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 vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2026-121965	Parse Server before 8.6.113 and 9.0.0 before 9.10.6-alpha.5 contains a prototype pollution vulnerability when building objects for Cloud Code triggers and LiveQuery, where a dot notation key whose intermediate segment resolves through an inherited member writes onto a process-wide built-in. Clients with write access to an object in a class with a trigger or LiveQuery can corrupt a built-in function, making unrelated requests fail until restart and denying service to all clients and hosted applications.	5.3	More Details
CVE-2026-120857	Missing Authorization vulnerability in VideoWhisper.com 2Way VideoCalls and Random Chat webcam-2way-videochat allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects 2Way VideoCalls and Random Chat: from n/a through 6.1.9.	5.3	More Details
CVE-2026-121571	Missing Authorization vulnerability in WP Desk Autopay dla WooCommerce pay-wp allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Autopay dla WooCommerce: from n/a through 2.3.0.	5.3	More Details
CVE-2026-123148	Missing Authorization vulnerability in TMS IvyForms ivyforms allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects IvyForms: from n/a through 1.5.1.	5.3	More Details
CVE-2026-121938	langchain4j-aideepin before 3.31.0 contains an insecure direct object reference vulnerability that allows authenticated users to read other users' character-chat conversations by supplying their character uuid. Attackers can request GET /character/{uuid}, which CharacterService.detail resolves without an ownership check, to obtain victims' questions, AI answers, and attachment and audio URLs.	5.3	More Details
CVE-2026-122139	blueprintUE Self-Hosted Edition before 4.3.3 contains an account enumeration vulnerability in ForgotPasswordMiddleware.php that allows unauthenticated attackers to identify registered email addresses. Attackers can compare password reset redirect targets for submitted emails, and failed lookups are never rate-limited, enabling unlimited enumeration attempts.	5.3	More Details
CVE-2026-123469	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Liquid Web / StellarWP The Events Calendar the-events-calendar allows Code Injection.This issue affects The Events Calendar: from n/a through 6.18.3.	5.3	More Details
CVE-2026-86795	The Community Events WordPress plugin before 1.6.0 does not have authorisation or nonce checks in one of its AJAX actions, allowing unauthenticated users to retrieve details of event submissions awaiting moderation, which are not available anywhere on the public site.	5.3	More Details
CVE-2026-122154	A vulnerability was found in purocean Yank Note 3.93.0. This impacts the function config.getAll of the file src/main/server/index.ts of the component Settings Endpoint. The manipulation results in information disclosure. The attack may be launched remotely. The exploit has been made public and could be used. Upgrading to version 3.93.1 will fix this issue. The patch is identified as 59f85d48f17a70a402ad59dcecacdbec20f954df. The affected component should be upgraded. The commit removes the key from the response.	5.3	More Details

CVE-2026-47738	liboqs is a C-language cryptographic library that provides implementations of post-quantum cryptography algorithms. Prior to 0.16.0, OQS_KEM_encaps_derand can dereference an uninitialized encaps_derand function pointer when called on NTRU-HPS-2048-509, NTRU-HPS-2048-677, NTRU-HPS-4096-821, NTRU-HPS-4096-1229, NTRU-HRSS-701, or NTRU-HRSS-1373. The affected NTRU constructors omit the OQS_KEM.encaps_derand member because those schemes do not support derandomized encapsulation, OQS_KEM objects are allocated without zero initialization, and the wrapper in src/kem/kem.c checks only that the OQS_KEM pointer is non-null before calling through the residual heap value. An application is affected only if it instantiates one of those six NTRU KEMs and invokes OQS_KEM_encaps_derand on it. The supported impact is a calling-process crash and denial of service. This issue is fixed in version 0.16.0.	5.3	More Details
CVE-2026-119502	Missing Authorization vulnerability in BdThemes Ultimate Store Kit Elementor Addons ultimate-store-kit allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Ultimate Store Kit Elementor Addons: from n/a through 4.0.1.	5.3	More Details
CVE-2026-107774	The Dokan: AI Powered WooCommerce Multivendor Marketplace Solution WordPress plugin before 5.3.3 does not use a trusted site-owned sender address when relaying its store contact form, instead placing the unauthenticated submitter's supplied address directly in the message's From header rather than a Reply-To, allowing unauthenticated attackers to make the site email its own vendors with the sender spoofed to an address at the site's own domain (such as its administrator), aligned with the domain's own SPF/DKIM.	5.3	More Details
CVE-2026-105971	The Car Dealer (Dealership) and Vehicle sales WordPress plugin through 4.73 does not restrict its unauthenticated single-listing AJAX action to published content, allowing an unauthenticated attacker to read the title, content and metadata of any private, draft, pending, future or trashed post by supplying its numeric id.	5.3	More Details
CVE-2026-119507	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in WPDeveloper NotificationX notificationx allows Code Injection.This issue affects NotificationX: from n/a through 3.3.6.	5.3	More Details
CVE-2026-33965	An attacker may send a malicious IMS message to the target device, potentially leading to information exposure through the SIP message flow.	5.3	More Details
CVE-2026-119511	Missing Authorization vulnerability in Saeed MC Woocommerce Wishlist smart-wishlist-for-more-convert allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects MC Woocommerce Wishlist: from n/a through 2.0.3.	5.3	More Details
CVE-2026-104254	liboqs is a C-language cryptographic library that provides implementations of post-quantum cryptography algorithms. From 0.11.0 through 0.16.0, builds configured with OQS_ENABLE_SIG_STFL_LMS=ON can read beyond a caller-supplied signature buffer when an untrusted truncated LMS or HSS-LMS signature reaches OQS_SIG_STFL_verify or OQS_SIG_STFL_alg_lms_verify. In hss_validate_signature_init() in src/sig_stfl/lms/external/hss_verify_inc.c, consumed-length checks do not ensure that the bottom-level q and C fields remain available, allowing up to 32 bytes to be read past the buffer. In version 0.16.0, is_hss_public_key() also reads at offset 8 after only a four-byte length check, allowing an over-read of up to eight bytes. No valid signature is required, but the public key must be syntactically plausible. The read data is consumed only by an internal hash and is not exposed, so the supported impact is a possible verifier crash and denial of service, not memory disclosure or acceptance of an invalid signature. This issue is scheduled to be fixed in version 0.17.0.	5.3	More Details
CVE-2026-103022	Urwid is a console user interface library for Python. Prior to 4.0.7, handle_short_request() in urwid/display/web.py performs unguarded character encoding on POST input and unguarded UTF-8 decoding on polling update socket output. A remote attacker who obtains a valid X-Urwid-ID session token can submit non-ASCII POST data that raises UnicodeEncodeError, while non-UTF-8 polling output raises UnicodeDecodeError, causing the CGI handler to return an error and terminate request processing. The POST exception path also leaves an opened file descriptor unclosed for the CGI process lifetime, so repeated requests can cause denial of service for the web display interface. This issue is fixed in version 4.0.7.	5.3	More Details
CVE-2026-122146	A weakness has been identified in 101arrowz fflate up to 0.8.3. This issue affects the function unzipSync of the file esm/index.mjs. This manipulation causes uncontrolled memory allocation. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks. It is suggested to update the configuration settings. The maintainer disputes this issue as a vulnerability. The library is a pure JavaScript decompressor that allocates memory proportional to the decompressed payload size, which is expected behavior. Excessive allocations simply throw a standard JavaScript RangeError or reach engine heap limits. Furthermore, because a low-level decompression library cannot distinguish between a maliciously crafted compression bomb and a legitimate file with a high compression ratio, the API explicitly provides a filter option allowing callers to restrict decompressed file sizes and prevent denial-of-service according to their application's requirements, as seen both in the documentation and noted in the reported issue.	5.3	More Details
CVE-2026-66987	HCL AION is affected by a vulnerability where the account lockout mechanism did not sufficiently restrict repeated failed login attempts, allowing an attacker to make a large number of password guesses against a user account. This may increase the risk of account compromise through brute-force attacks, potentially resulting in unintended behavior or security impact under certain conditions.	5.3	More Details
CVE-2026-	WWBN AVideo 29.0 through 29.4.0 contains a race condition vulnerability in plugin/PayPalYPT/ipn.php that allows attackers to bypass IPN replay protection due to a non-atomic deduplication check and insert. Attackers can concurrently replay a captured valid recurring-payment notification so both requests pass	5.3	More Details

123486	isRecurringPaymentIdUsed(), obtaining duplicate wallet credits and subscription renewals.		
CVE-2026-97702	Open edX Platform enables the authoring and delivery of online learning at any scale. From the Ulmo release until release/ulmo.4 and release/verawood.1, the GET /api/support/v1/manage_course_team/ endpoint in CourseTeamManageAPIView requires only IsAuthenticated and omits the global support-role authorization check intended for this help-desk surface. Any authenticated learner can supply an email, username, or user_id for an arbitrary target and use the 200 and 404 response discrepancy to distinguish an active account from an absent or inactive account. A caller with a course-level or organization-level instructor role can additionally obtain the target user's staff or instructor assignments within the caller's course or organization scope. Anonymous callers remain blocked, and the separately authorized PUT behavior is outside this vulnerability. This issue is fixed in release/ulmo.4 and release/verawood.1.	5.3	More Details
CVE-2026-120548	The YML for Yandex Market plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 5.10.0 via the 'y4ym_check_action' parameter. This makes it possible for unauthenticated attackers to extract the merchant's plaintext Yandex Market API key written to the publicly accessible log file at wp-content/uploads/y4ym/yml-for-yandex-market.log, granting full control over the merchant's marketplace catalogue, prices, and stock. Exploitation requires that the targeted feed has a stored Yandex Market API key and that the y4ym_keeplogs option is enabled — both conditions that represent normal, documented plugin usage actively encouraged by the plugin's own support and feedback workflow.	5.3	More Details
CVE-2026-123617	Openwhyd before 1.65.1 contains a NoSQL injection vulnerability that allows unauthenticated attackers to manipulate user lookups by passing JSON objects in the id parameter. Attackers can send MongoDB query operators such as $ne or $gt to POST /api/user to select and enumerate other users' public profile records.	5.3	More Details
CVE-2026-62365	Wazuh is an open-source security platform providing unified XDR and SIEM protection for endpoints and cloud workloads. DecodeWinevt in src/analysisd/decoders/winevtchannel.c accumulates unnamed Windows EventChannel Data element contents into the fixed 65,535-byte join_data heap buffer but passes the growing content length, rather than the OS_MAXSTR buffer capacity, as the snprintf size. An enrolled agent can submit an EventChannel message containing four maximum-sized unnamed Data elements, causing the fourth accumulation to write beyond join_data and corrupt adjacent heap metadata. The subsequent free of join_data2 causes the wazuh-analysisd process to terminate, stopping log ingestion for all agents handled by that manager. This vulnerability is fixed in 4.14.7.	5.3	More Details
CVE-2026-120852	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Brainstorm Force CartFlows cartflows allows Code Injection.This issue affects CartFlows: from n/a through 3.3.0.	5.3	More Details
CVE-2026-120853	Missing Authorization vulnerability in Brainstorm Force CartFlows cartflows allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects CartFlows: from n/a through 3.3.0.	5.3	More Details
CVE-2026-123466	Missing Authorization vulnerability in LeapWorx Premium Blocks – Gutenberg Blocks for WordPress premium-blocks-for-gutenberg allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Premium Blocks – Gutenberg Blocks for WordPress: from n/a through 2.3.18.	5.3	More Details
CVE-2026-123676	A vulnerability has been found in xxyopen/201206030 novel up to 3.5.0. This impacts the function BookServiceImpl.getBookContentAbout of the file src/main/java/io/github/xxyopen/novel/service/impl/BookServiceImpl.java of the component Book Content Service. Such manipulation of the argument chapterId leads to improper authorization. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The name of the patch is 966c4bdde3521dc0a165d15a2acff66ee33eaaa7. Applying a patch is advised to resolve this issue.	5.3	More Details
CVE-2026-121536	The WP Data Access – App Builder for Tables, Forms, Dashboards, Charts & Maps plugin for WordPress is vulnerable to generic SQL Injection via the 'engine' parameter in all versions up to, and including, 5.5.90 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 is only exploitable when an administrator has configured a Data Project page to admit a lower-privileged role, which is the plugin's documented mechanism for sharing projects with subscribers and other users.	5.3	More Details
CVE-2026-90964	The Essential Real Estate WordPress plugin before 5.3.5 does not restrict the recipient of one of its contact email actions, allowing unauthenticated users to send emails to arbitrary addresses with an attacker-controlled sender header and message body through the site.	5.3	More Details
CVE-2026-97371	ntopng is a web-based network traffic monitoring application. Prior to 6.7.260721, ndpi_get_custom_category_match writes a four-byte nDPI protocol-category value through a pointer to the two-byte id variable in IpAddress::reloadBlacklist in src/IpAddress.cpp during packet dissection and host initialization. A remote unauthenticated attacker on a monitored network segment can send packets that match custom-category rules, causing stack corruption and denial of service without user interaction. This issue is fixed in version 6.7.260721.	5.3	More Details
CVE-	ASN1SCC is an open source ASN.1 compiler for embedded systems. Prior to 4.7.0.1, the ACN runtime function Acn_Dec_String_CharIndex_private in asn1crt/asn1crt_encoding_acn.c and the generated uPER decoder InternalItem_string_with_alpha_decode in StgC/uper_c.stg do not validate a decoded character index before		More

2026-75615	reading allowedCharSet. For string alphabets whose size is not a power of two, a crafted message can select an unused encoded index, read a small bounded window of adjacent static program constants, and return the byte as a successfully decoded character. The full 128-character IA5String alphabet is not affected. This issue is fixed in version 4.7.0.1.	5.3	Details
CVE-2026-121633	The Order Tracking WordPress plugin before 3.6.0 does not verify that a PayPal payment notification was sent to the merchant's account, or that its amount matches the order total, before marking an order as paid, which could allow unauthenticated attackers to mark arbitrary orders as paid using a trivial payment to their own PayPal account.	5.3	More Details
CVE-2026-112910	filelock is a platform-independent file lock for Python. From 3.10.0 until 4.2.1, filelock on Windows ignores the mode argument for WindowsFileLock files and the ReadWriteLock SQLite database. A lock created with mode=0o600 receives the parent directory's inheritable ACL because _open_non_reparse_fd and _nt_open do not create an owner-only security descriptor. Another local account with inherited access can read holder metadata or the lock database, modify those files where the ACL permits writes, or take the byte-range lock after release and delay later acquisitions. UnixFileLock is not affected, and mutual exclusion between cooperating processes continues to hold. This issue is fixed in version 4.2.1.	5.3	More Details
CVE-2026-123183	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in PluginUs.Net Active Products Tables for WooCommerce profit-products-tables-for-woocommerce allows Code Injection.This issue affects Active Products Tables for WooCommerce: from n/a through 2.1.6.	5.3	More Details
CVE-2026-17389	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote attacker to obtain sensitive information from the connected LDAP directory due to LDAP injection. Input is not properly neutralized in directory lookups, which could cause queries to return additional data.	5.3	More Details
CVE-2026-57775	Authentication Bypass Using an Alternate Path or Channel vulnerability in RelyWP Simple Cloudflare Turnstile simple-cloudflare-turnstile allows Authentication Abuse.This issue affects Simple Cloudflare Turnstile: from n/a through 1.44.1.	5.3	More Details
CVE-2026-123462	Missing Authorization vulnerability in myCred myCred mycred allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects myCred: from n/a through 4.0.2.	5.3	More Details
CVE-2026-27356	Missing Authorization vulnerability in ibericode MC4WP mailchimp-for-wp allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects MC4WP: from n/a through 4.14.1.	5.3	More Details
CVE-2026-116781	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to 1.11.2, ws_read_frame() unmasked a WebSocket payload by iterating wsh->datalen, which included frame headers, while indexing from the payload pointer. A masked frame filling the 64 KiB receive buffer could therefore XOR up to 14 bytes beyond the buffer, and the exact-capacity case also wrote a terminating NUL one byte out of bounds. The flaw is reachable before authentication when mod_xml_rpc and its opt-in WebSocket endpoint are enabled, while both features are disabled in the stock configuration. The writes remain within the same connection handle's adjacent outbound buffer, so neither a process crash nor cross-session disclosure has been demonstrated. This issue is fixed in version 1.11.2.	5.3	More Details
CVE-2026-106000	The Booking Package WordPress plugin before 1.7.34 does not require payment to be completed before saving a booking on calendars configured to require online payment, allowing unauthenticated users to create confirmed bookings without paying.	5.3	More Details
CVE-2026-110705	The Redux Framework plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 4.5.16. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to export the entire Redux options panel configuration — including API keys, SMTP credentials, licence keys, and third-party tokens — that is otherwise restricted to administrators. Exploitation requires that a theme or plugin registers a Redux import_export field on a user profile via Redux_Users::set_profile(), which causes the nonce to be printed into the subscriber's own /wp-admin/profile.php page source, making it directly readable without any additional privileges.	5.3	More Details
CVE-2026-112908	filelock is a platform-independent file lock for Python. From version 3.30.0 until version 4.2.1, StrictSoftFileLock and AsyncStrictSoftFileLock on POSIX systems create coordination and claim directories without applying the caller’s restrictive lock mode. A permissive umask or inherited default ACL can leave these directories writable by another local user, allowing that user to delete an active holder’s claims. Another authorized process can then acquire the lock while the original holder remains in its critical section. An attacker can also plant malformed claims to prevent acquisition. This issue is fixed in version 4.2.1.	5.3	More Details
CVE-2026-123860	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Crocoblock JetFormBuilder jetformbuilder allows Code Injection.This issue affects JetFormBuilder: from n/a through 3.6.8.	5.3	More Details
CVE-2026-121575	Missing Authorization vulnerability in WP User Manager WP User Manager wp-user-manager allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP User Manager: from n/a through 2.10.4.	5.3	More Details

CVE-2026-119259	The All-in-One Video Gallery WordPress plugin before 5.1.0 does not check the type, status or ownership of the target post before writing its view count and duration meta, allowing unauthenticated visitors to create or change that meta on any post, including private and draft posts, and to inflate the view count without limit.	5.3	More Details
CVE-2026-100362	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Prior to 7.15.2 and 8.10.2, the /legacy/Api/V8/OAuth2 password-grant endpoint returns distinct error messages for an invalid username and an invalid password. An unauthenticated remote attacker can use those response differences to enumerate valid CRM usernames and target confirmed accounts with password spraying, credential stuffing, brute-force, or social-engineering attacks. This issue is fixed in versions 7.15.2 and 8.10.2.	5.3	More Details
CVE-2026-16711	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote attacker to inject platform credentials into outbound requests due to improper input validation. A validation check is not sufficiently strict, which could cause platform credentials to be included in outbound requests.	5.3	More Details
CVE-2026-118167	The MC4WP: Mailchimp for WordPress plugin before 4.15.0 does not validate that the Mailchimp audience a sign-up form or bundled integration subscribes a visitor to matches the audience configured by the site owner, allowing unauthenticated visitors to subscribe arbitrary email addresses to any other audience in the site's connected Mailchimp account.	5.3	More Details
CVE-2026-123483	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Crocoblock JetFormBuilder jetformbuilder allows Code Injection.This issue affects JetFormBuilder: from n/a through 3.6.8.	5.3	More Details
CVE-2026-118523	The EventPrime WordPress plugin before 4.3.6.1 does not keep the built-in Pending Review post status non-public, allowing unauthenticated users to view posts, pages and other content that are awaiting review.	5.3	More Details
CVE-2026-112244	The Duplicator WordPress plugin before 5.1.0, duplicator-pro WordPress plugin before 5.1.0 does not prevent direct access to some of its bundled PHP files, which initialise without their expected context, trigger a fatal error, and return a stack trace that discloses the server's absolute filesystem paths to unauthenticated users.	5.3	More Details
CVE-2026-118404	The Premium Packages WordPress plugin before 7.3.1 does not verify ownership or session binding when loading a previously saved shopping cart, allowing any unauthenticated user who obtains another shopper's saved-cart identifier to load that shopper's cart contents, including selected products, quantities and buyer-entered custom field data, into their own session.	5.3	More Details
CVE-2026-123474	Missing Authorization vulnerability in LeapWorx Premium Blocks – Gutenberg Blocks for WordPress premium-blocks-for-gutenberg allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Premium Blocks – Gutenberg Blocks for WordPress: from n/a through 2.3.18.	5.3	More Details
CVE-2026-112899	Pillow is a Python imaging library. In versions 2.3.0 through 12.3.0, EPS rendering does not validate the scaled image dimensions before invoking Ghostscript. Applications that process untrusted EPS or PostScript files using an application-selected scale greater than one can incur excessive Ghostscript CPU and temporary disk consumption. In versions with decompression-bomb protection, the scaled output is checked only after Ghostscript has completed rendering, allowing resource consumption beyond the configured pixel limit. The amplification depends on the scale selected by the application, not an attacker-controlled scale value. This issue is fixed in version 13.0.0.	5.3	More Details
CVE-2026-120555	The Jupiter X Core plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 4.62.0 via the 'file' 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 path confinement check introduced in the CVE-2023-3813 fix (strpos + realpath) is present and working, so reads are confined to wp-content/uploads/ and cannot reach wp-config.php or other files outside that directory.	5.3	More Details
CVE-2026-121775	Missing Authorization vulnerability in VillaTheme CURCY woo-multi-currency allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects CURCY: from n/a through 2.2.20.	5.3	More Details
CVE-2026-120520	The Greenshift – animation and page builder blocks plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 13.2.2 via the 'img (or any key the publisher references in {{GET:key}})' parameter. This makes it possible for unauthenticated attackers to extract authenticated users' HttpOnly WordPress session cookies, specifically wordpress_logged_in_* tokens, by injecting a nested {{COOKIE:}} placeholder via a GET parameter that causes the victim's browser to transmit the cookie value to an attacker-controlled host as an image src URL. Exploitation requires that a site publisher has configured a public GreenShift Element image block whose src attribute contains a {{GET:}} placeholder, and that a logged-in user can be induced to open the attacker's crafted link — neither condition is part of the plugin's default state.	5.3	More Details
CVE-2026-122326	Chevereto before 4.5.8 contains an authorization bypass vulnerability in the get-album-contents action of the /json route that allows unauthenticated attackers to list private albums by supplying another user's album id. Attackers with a session token from any public page and an album's encoded id can obtain image filenames, viewer and direct file URLs, and download private images.	5.3	More Details
CVE-2026-17202	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote attacker to enumerate usernames due to observable differences in response behavior.	5.3	More Details

CVE-2026-121636	The Quick Event Manager WordPress plugin before 9.19 does not verify the authenticity of PayPal payment notifications before marking event registrations as paid, which could allow unauthenticated attackers to mark registrations as paid without making a payment.	5.3	More Details
CVE-2026-119751	Content Egg plugin for WordPress before 12.1.0 contains a broken access control vulnerability that allows unauthenticated attackers to retrieve Content Egg product data from unpublished posts by calling the REST route POST /wp-json/content-egg/v1/render-blocks, whose permission_check() improperly returns true when no X-WP-Nonce header is supplied. Attackers can supply the post_id and module id of a draft, pending, scheduled, or private post to handle_render(), which lacks a publish-status check, to disclose product titles, destination and affiliate URLs, merchant or domain information, and descriptions.	5.3	More Details
CVE-2026-121618	A weakness has been identified in Linksys E5600 1.1.0.26. This affects an unknown part of the file /cgi-bin/fqc.cgi of the component Factory Quality Control. This manipulation causes information disclosure. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way. This vulnerability only affects products that are no longer supported by the maintainer.	5.3	More Details
CVE-2026-121589	A weakness has been identified in spatie url-signer up to 2.1.3. Affected is the function AbstractUrlSigner::validate of the file AbstractUrlSigner.php of the component URL Validation. This manipulation of the argument expires causes incorrect type conversion. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks. Upgrading to version 2.1.4 is able to address this issue. Patch name: 86af3355388210668f6bfbe9007bd6545d4942ad. It is recommended to upgrade the affected component.	5.3	More Details
CVE-2026-115257	The WP Roster WordPress plugin before 2.36 does not perform any capability or nonce checks before writing its stored roster data, allowing unauthenticated attackers to overwrite, wipe or restore the content of any roster.	5.3	More Details
CVE-2026-121492	The Fiber Admin WordPress plugin before 4.0.1 does not have authorisation checks in some of its AJAX actions, allowing unauthenticated users to change the order of arbitrary posts, including drafts, private posts and navigation menu items, as well as the order of taxonomy terms when term ordering is enabled.	5.3	More Details
CVE-2026-121777	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Cool Plugins Cool Formkit Lite extensions-for-elementor-form allows Code Injection.This issue affects Cool Formkit Lite: from n/a through 2.7.10.	5.3	More Details
CVE-2026-123197	WPPConnect Server through 2.10.76 contains a missing authentication vulnerability that allows unauthenticated attackers to read decrypted sticker media through the /files static mount. Attackers can enumerate Unix timestamps in GET /files/file<timestamp>.webp requests to retrieve stickers from any session, bypassing per-session token checks.	5.3	More Details
CVE-2026-17098	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote attacker to obtain sensitive information due to verbose error messages.	5.3	More Details
CVE-2026-122663	Missing Authorization vulnerability in VillaTheme CURCY woo-multi-currency allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects CURCY: from n/a through 2.2.20.	5.3	More Details
CVE-2026-123201	Buku (bukuserver) through 5.1.1 contains an unauthenticated server-side request forgery vulnerability that allows remote attackers to make the server request internal hosts by supplying a url parameter to /api/fetch_data or /api/network_handle. Attackers can target loopback, private, or cloud metadata IP addresses, which pass the weak is_bad_url() check and follow redirects, to discover internal services and read their page titles, descriptions, and keywords.	5.3	More Details
CVE-2026-121616	A vulnerability was identified in Linksys E5600 1.1.0.26. Affected by this vulnerability is the function strcpy of the file /cgi-bin/mesh_login.cgi of the component JSON Request Parser. The manipulation of the argument username/password/token/source/cn/action leads to out-of-bounds write. The attack may be initiated 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. This vulnerability only affects products that are no longer supported by the maintainer.	5.3	More Details
CVE-2026-121380	The Tournamatch WordPress plugin before 4.7.1 does not restrict access to its team invitation listing, allowing unauthenticated users to retrieve the email addresses of people invited to join teams.	5.3	More Details
CVE-2026-17393	IBM API Connect 10.0.8.0 through 10.0.8.12 could allow a local attacker to obtain sensitive information due to the use of a cryptographically weak pseudo-random number generator.	5.1	More Details
CVE-	liboqs is a C-language cryptographic library that provides implementations of post-quantum cryptography algorithms. Prior to 0.16.0, the ct_select function in src/kem/frodokem/external/util.c for the FrodoKEM-640, FrodoKEM-976, and FrodoKEM-1344 AES and SHAKE reference variants lacks a value barrier in the Fujisaki-Okamoto implicit-rejection path. When compiled with Clang 17 or later at an affected optimization level such as -Os, the compiler can emit a secret-dependent conditional load, causing the real and rejection secret paths to		More

2026-44519	leave distinguishable cache residency after successful and failed decapsulation. A local attacker able to perform repeated cache-timing measurements may use this oracle as part of a private-key recovery attack. Default -O3 builds vectorize both source loads and do not exhibit the reported behavior, and the advisory does not report the same generated memory-access pattern in NTRU, NTRU-Prime, BIKE, HQC, Classic McEliece, Kyber, or the already-barriered ML-KEM implementation. This issue is fixed in version 0.16.0.	5.1	Details
CVE-2026-19703	A weak password hashing vulnerability has been identified on SonicOS virtual appliances, which in specific conditions could potentially enable an attacker with existing local access to disclose a platform credential. The credential provides access to a limited subset of platform settings.	5.1	More Details
CVE-2026-118530	The Directorist: AI-Powered Business Directory, Listings & Classified Ads WordPress plugin before 8.11 does not check that the acting user may edit each targeted user when handling an email-verification bulk action on multisite, allowing an Administrator of one site on the network to lock out users of other sites, including the network Super Administrator, until they re-verify their email.	5.0	More Details
CVE-2026-17064	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to an insecure direct object reference.	5.0	More Details
CVE-2026-123973	SharePoint Products CopyMove before 2026-11-06 allows traversal. An authenticated SharePoint user with the necessary permissions to use the ZIP import functionality may exploit a path traversal vulnerability in CopyMove for SharePoint 2019 and CopyMove for SharePoint V6 by supplying a crafted ZIP archive. A path traversal vulnerability in the ZIP import functionality of SharePoint Products ApS CopyMove for SharePoint 2019 and CopyMove for SharePoint V6 allows a user with access to the ZIP import functionality to supply a crafted ZIP archive containing malicious entry paths. During extraction, these paths may cause files to be written outside the intended extraction directory. The issue has been addressed by implementing ZIP archive entry path validation to prevent extraction outside the designated directory.	5.0	More Details
CVE-2026-88983	Kubeflow Pipelines enables users to build and deploy portable, scalable machine learning workflows. Prior to 2.17.0, the API server's pipeline and pipeline-version creation paths fetch a caller-supplied pipelineURL without restricting the destination. An authenticated caller with permission to create a pipeline or pipeline version can make requests from the API server to internal services and observe a limited status-code oracle. Arbitrary response-body disclosure, credential theft, and integrity or availability impact are not established. This issue is fixed in version 2.17.0.	5.0	More Details
CVE-2026-17314	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to server-side request forgery.	5.0	More Details
CVE-2026-102356	Kroki creates diagrams from textual descriptions. From 0.26.0 until 0.31.2, the optional Mermaid companion's mermaid/src/worker.js renders attacker-controlled flowchart image nodes in headless Chromium without a network request policy, even when KROKI_SAFE_MODE is set to secure. An actor who can submit Mermaid source and satisfy any authentication or authorization configured by the deployment can cause the companion to issue HTTP or HTTPS GET requests when requesting PNG output. Exploitation requires the Mermaid companion, PNG rendering through its headless Chromium process, a diagram-submission path available to the actor, and network reachability from the companion to the target. The demonstrated impact is limited to blind request reachability and possible state-changing GET endpoints; response exfiltration, cloud metadata access, port scanning, and access beyond the companion's network reachability are not established. This issue is fixed in version 0.31.2.	5.0	More Details
CVE-2026-85351	The FV Flowplayer Video Player WordPress plugin before 7.5.56.7212 does not validate a user-supplied URL before performing a server-side fetch whose response body is stored and served publicly, allowing users with Contributor-level access and above to perform Server-Side Request Forgery (SSRF) attacks and to read the response of an internal resource when it is returned with an image content type.	5.0	More Details
CVE-2026-17366	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to broken object-level authorization.	5.0	More Details
CVE-2026-123277	In JetBrains CLion before 2026.3, 2026.2.4.1 missing authentication allowed local users to obtain the debug session environment on Linux	5.0	More Details
CVE-2026-17302	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to probe internal network services due to improper validation of a user-supplied URL.	5.0	More Details
CVE-2026-17371	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to broken object-level authorization.	5.0	More Details
CVE-2026-17377	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to forge audit records due to improper output neutralization for logs.	5.0	More Details

CVE-2026-123298	In JetBrains Hub before 2026.2.52556 sMTP command injection via email verification was possible	5.0	More Details
CVE-2026-122008	Oqtane Framework before 10.3.0 contains a server-side request forgery vulnerability in the UploadFile endpoint of FileController.cs that allows authenticated registered users to make the server fetch arbitrary URLs by supplying a caller-controlled url parameter to HttpClient.GetStreamAsync without validating the scheme, host, or IP address. Attackers can request internal resources such as cloud instance metadata services or localhost-bound management interfaces, save the fetched response as a file in their own user folder, and retrieve it via the download endpoint to exfiltrate sensitive internal data or enumerate internal network hosts and ports.	5.0	More Details
CVE-2026-17428	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to improper authorization. Values supplied in the request URL are used in authorization decisions without sufficient verification, which could allow access to information belonging to others.	5.0	More Details
CVE-2026-119211	The AAA Autoload Optimizer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'option_page' parameter in all versions up to, and including, 1.7.0 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. Exploitation requires the plugin's Option Tracking setting to be configured to 'Legacy' mode, and succeeds despite WordPress ultimately returning HTTP 403 to the low-privileged caller because the vulnerable 'all' filter fires before the capability check in wp-admin/options.php.	4.9	More Details
CVE-2026-118056	The Image Hover Effects Ultimate (Image Gallery, Effects, Lightbox, Comparison & Magnifier) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'rawdata.oxi_image_comparison_before_text' parameter in all versions up to, and including, 9.12.2 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 is only exploitable when an administrator has configured the plugin's "Who can edit" setting to Subscriber, which allows any authenticated user to overwrite existing styles — including those created by administrators — via a missing ownership check on the target style ID.	4.9	More Details
CVE-2026-84161	When an operator enables store.analysis_statistics_dir, a network client with PRODUCT_STORE permission for a product can call that product's storeAnalysisStatistics Thrift-over-HTTP method. CodeChecker 6.29.0 decodes the attacker-controlled Base64 string and passes the complete compressed input to one-shot zlib.decompress(). No maximum decompressed size is enforced. This gives a correctly authorized, non-superuser store account a high-ratio memory and persistent-disk amplification primitive. The complete output is first materialized as a Python bytes object and is then written to the configured statistics directory. A sufficiently scaled payload can exhaust the API worker or host memory and impair CodeChecker availability. The shipped value of store.analysis_statistics_dir is null, so the affected feature is disabled by default. The primary assessment does not rely on authentication being disabled. There is no authorization bypass and no path traversal in this report.	4.9	More Details
CVE-2026-109977	The YaySMTP – WP Mail SMTP with Email Logs, Tracking & Reports plugin for WordPress is vulnerable to time-based SQL Injection via the 'params[searchKey]' parameter in all versions up to, and including, 2.7.8 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	4.9	More Details
CVE-2026-123492	SiYuan before 3.8.9 contains a nil pointer dereference vulnerability in privateCacheMiddleware that allows authenticated attackers to crash the kernel by reading nonexistent MCP resources. Attackers with a valid API token can send a resources/read request in an initialized MCP session, causing a panic that terminates the kernel process and interrupts service.	4.9	More Details
CVE-2026-118186	The PublishPress Revisions: Duplicate Posts, Submit, Approve and Schedule Content Changes WordPress plugin before 4.3.1 does not correctly restrict who may publish content, allowing users such as Contributors who can edit but not publish to make unreviewed posts and pages publicly live, bypassing the intended editorial approval workflow.	4.9	More Details
CVE-2026-121967	Coder 2.28.0 before 2.29.22, 2.30.0 before 2.34.13, 2.35.0 before 2.35.10, 2.36.0 before 2.36.8, 2.37.0 before 2.37.5, and 2.38.0 before 2.38.1 contains a path traversal vulnerability in the AI Gateway passthrough router, which forwards percent-encoded dot segments upstream without rejecting them. Authenticated users can send paths such as %2e%2e or ..%2F under allowlisted prefixes to reach unintended provider endpoints using the deployment's centrally managed provider key.	4.9	More Details
CVE-2026-112334	Wazuh from 1.0.0 before 4.14.9 contains an out-of-bounds write vulnerability in wazuh-execd that allows privileged manager-configuration attackers to corrupt root process memory via excess ar.conf entries. Attackers controlling ossec.conf active-response blocks can push over 64 commands to agents, overflowing ReadExecConfig() arrays and crashing Active Response fleet-wide.	4.9	More Details
CVE-2026-	A flaw was found in the SAML brokering component of Keycloak, an identity and access management solution. The issue occurs when Keycloak acts as an intermediary between an upstream identity provider and downstream services. Keycloak fails to respect specific security instructions called ProxyRestrictions in the login messages it	4.9	More

92856	receives. This allows a user to log into downstream services even when the original identity provider explicitly forbade further sharing of the login session. As a result, users can bypass security boundaries intended to limit where their identity can be used.		Details
CVE-2026-115262	The Duplicator WordPress plugin before 5.1.0, duplicator-pro WordPress plugin before 5.1.0 does not restrict its database charset and collation rewrite to schema statements during a restore, so a value a Subscriber stores in their own profile can break out of its string literal and inject SQL into the restore's INSERT statement when an administrator restores the backup onto a server lacking one of the source's charsets or collations.	4.8	More Details
CVE-2026-35111	HCL AION is affected by a vulnerability where the Cross-Origin-Resource-Policy (CORP) header was missing or insecure, allowing application resources to be loaded by other origins. This may expose resources to cross-origin data leakage, potentially resulting in unintended behavior or security impact under certain conditions.	4.8	More Details
CVE-2026-17214	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote attacker to bypass security restrictions due to LDAP injection.	4.8	More Details
CVE-2026-121943	Irontec sngrep through 1.9.0 contains an out-of-bounds stack read vulnerability in sip_check_packet and sip_validate_packet caused by an off-by-one length check on 10240-byte SIP payloads. Remote attackers can send a crafted UDP or TCP SIP packet or supply a pcap file to crash sngrep or leak adjacent stack bytes into displayed SIP fields.	4.8	More Details
CVE-2026-87043	The entropy-device random number generator in subsys/random/random_entropy_device.c returned early with -ENODEV from rand_get() as soon as device_is_ready() failed, before reaching the non-cryptographic system-timer fallback further down the same function. Because z_impl_sys_rand_get() returns void and discards that error — and the public sys_rand_get() syscall is itself declared void, so it cannot report failure — the caller's output buffer was left untouched and its previous contents were handed back as random data. The thin wrappers make this a plain uninitialized read: sys_rand32_get() declares uint32_t ret;, calls sys_rand_get(&ret, sizeof(ret)) and returns ret. The "not ready" state is a normal runtime condition rather than a fault. Entropy drivers initialise at PRE_KERNEL_1 with CONFIG_ENTROPY_INIT_PRIORITY (default 50), so any earlier initialiser — kernel objects run at priority 30 — observes an unready device; the sibling generator subsys/random/random_xoshiro128.c and z_early_rand_get() in kernel/init.c both already carried an explicit timer fallback for exactly this case. The state is also permanent for the boot when an entropy driver's init hook fails, which several in-tree drivers can do on real hardware (entropy_stm32 on an RNG clock configuration error, entropy_psa_crypto when psa_crypto_init() fails, entropy_nrf_cracen, entropy_esp32, entropy_virtio). When this occurs, every non-cryptographic random value in the system is either a constant or stale memory. coap_next_token() in subsys/net/lib/coap/coap.c fills a static buffer, so every CoAP token becomes the same .bss constant; tcp_init_isn() in subsys/net/ip/tcp.c returns an uninitialized stack word as the TCP initial sequence number; DHCPv4/DHCPv6 transaction IDs, WebSocket masking keys and RTP SSRCs are similarly degraded, and arch/arm64/core/pac.c derives per-thread Pointer Authentication keys from the same source. Where the bytes are transmitted directly — SSH packet padding, the netmidi2 session nonce, a DTLS connection ID on builds without CONFIG_CSPRNG_ENABLED — stale caller stack or heap contents are disclosed on the wire. The fix initialises ret to -ENODEV and only calls entropy_get_entropy() when the device is ready, so the not-ready case now falls through to the timer fallback and the buffer is always written. The cryptographically secure path is unchanged: sys_csrand_get() still propagates the error to the caller and never silently degrades. An attacker cannot induce the unready state, but can observe and exploit the resulting non-random values remotely on an affected device.	4.8	More Details
CVE-2026-118166	The MC4WP: Mailchimp for WordPress WordPress plugin before 4.15.0 does not prevent request-derived values in its dynamic content tags from being processed as shortcodes when a form is embedded with its block, allowing unauthenticated visitors to execute arbitrary registered shortcodes with attacker-chosen attributes. This requires the site owner to have added a request-derived tag to the form content and to embed the form with the block rather than the classic shortcode.	4.8	More Details
CVE-2026-54442	Emissary is a P2P based data-driven workflow engine. Prior to 8.51.0, the VALID_LINK validation in src/main/java/emissary/server/mvc/NavAction.java accepts protocol-relative URLs when processing configured navigation links. Browser URL normalization can interpret these accepted strings as external origins. The authoritative advisory attributes open redirect, server-side request forgery, and cloud metadata access to this bypass, but it identifies neither the server-side dereference path nor how navigation-link processing reaches that path. This issue is fixed in version 8.51.0.	4.8	More Details
CVE-2026-123318	In JetBrains Ktor before 3.6.1 hTTP request smuggling was possible in the CIO engine	4.8	More Details
CVE-2026-35113	HCL AION is affected by a vulnerability where the Cross-Origin-Opener-Policy (COOP) header was missing or insecure, allowing cross-origin documents to share a browsing context with the application. This may enable cross-window attacks, potentially resulting in unintended behavior or security impact under certain conditions.	4.8	More Details
CVE-2026-35102	HCL AION is affected by an open redirect vulnerability in the navigation bar of the GenAI web interface (Navbar component). The switch-version action redirected the browser to a dynamically constructed URL (window origin + '/workspace') without validating the redirect destination. This may be used in phishing attacks, potentially resulting in unintended behavior or security impact under certain conditions.	4.7	More Details
CVE-	In JetBrains IntelliJ IDEA before 2026.3 opening arbitrary URLs without confirmation was possible via the Remote		More

2026-123839	Development port forwarding model	4.7	Details
CVE-2026-123840	In JetBrains IntelliJ IDEA before 2026.3 hTML injection was possible in Remote Development editor tabs	4.7	More Details
CVE-2026-120509	The Real Testimonials – Testimonial Slider, Collect Customer Reviews and Video Testimonials plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'tpro_client_name' parameter in all versions up to, and including, 4.1.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Successful exploitation requires an administrator to publish the submitted testimonial, trigger the Show Preview AJAX handler, and save an Update, which canonicalizes and persists the attacker-controlled payload as the Manage View title — matching the plugin's standard moderation workflow. Successful exploitation additionally requires an action by an administrator — the attacker cannot trigger the vulnerability on their own.	4.7	More Details
CVE-2026-122158	A security flaw has been discovered in InvoiceShelf up to 2.4.3/3.0.0-alpha.3. Affected by this issue is the function MemberService::create of the file app/Domains/Accounts/Application/MemberService.php. Performing a manipulation of the argument companies[].id/companies[].role results in improper access controls. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks. Upgrading to version 2.4.4 and 3.0.0-alpha.4 can resolve this issue. The patch is named c798b513c3ab6e672a1678774720fbb282f4d0c6. It is recommended to upgrade the affected component.	4.7	More Details
CVE-2026-35103	HCL AION is affected by an open redirect vulnerability on the role assignment pending page (RoleAssignPending component). The redirect to the login page used a URL taken from build configuration (NEXT_PUBLIC_LOGIN_URL) without validating the redirect destination. This may be used in phishing attacks, potentially resulting in unintended behavior or security impact under certain conditions.	4.7	More Details
CVE-2026-35104	HCL AION is affected by an open redirect vulnerability on the user registration page (Signup component). The redirect performed after registration used the value of the 'redirect' query parameter without validation, so a crafted registration link could send a user to an untrusted external site. This may be used in phishing attacks, potentially resulting in unintended behavior or security impact under certain conditions.	4.7	More Details
CVE-2026-35105	HCL AION is affected by an open redirect vulnerability in the session-handling logic of the GenAI web interface (UserContext component, line 78). The redirect to the login page used a URL taken from build configuration (NEXT_PUBLIC_LOGIN_URL) without validating the redirect destination. This may be used in phishing attacks, potentially resulting in unintended behavior or security impact under certain conditions.	4.7	More Details
CVE-2026-35106	HCL AION is affected by an open redirect vulnerability in the session-handling logic of the GenAI web interface (UserContext component, line 89). A second redirect to the login page in this component used a URL taken from build configuration (NEXT_PUBLIC_LOGIN_URL) without validating the redirect destination. This may be used in phishing attacks, potentially resulting in unintended behavior or security impact under certain conditions.	4.7	More Details
CVE-2026-35107	HCL AION is affected by an open redirect vulnerability in the user menu of the GenAI web interface (UserMenu component). The redirect to the login page on logout used a URL taken from build configuration (NEXT_PUBLIC_LOGIN_URL) without validating the redirect destination. This may be used in phishing attacks, potentially resulting in unintended behavior or security impact under certain conditions.	4.7	More Details
CVE-2026-123332	In JetBrains YouTrack before 2026.2.19562 missing authorization allowed Project Admin to manage VCS hosting server configurations	4.7	More Details
CVE-2026-122234	jsondiffpatch before 0.7.7 contains a cross-site scripting vulnerability that allows attackers to inject markup by supplying an unescaped array-move destination index in a delta. Attackers who control a delta passed to formatters.html.format() or formatters.annotated.format() can embed script that executes in the application's origin when output is rendered.	4.7	More Details
CVE-2026-120477	The Stop Spammers Classic plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'author' POST parameter in versions up to, and including, 2026.6. An unauthenticated POST handled on init stores the attacker-supplied author field (after sanitize_text_field, which does not escape single quotes) into the ss_stop_sp_reg_stats option history. The Log Report admin page then renders that stored value inside a single-quoted JavaScript string within a double-quoted onclick attribute using esc_js(); because esc_js() uses _wp_specialchars with ENT_COMPAT it does not escape single quotes, allowing the stored value to break out of the JS string literal and inject arbitrary JavaScript. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute whenever an administrator with manage_options access clicks the 'Report to SFS' link on an attacker-poisoned log row (the StopForumSpam API key must be configured for that link to be rendered — the field is empty by default). Successful exploitation additionally requires an action by an administrator — the attacker cannot trigger the vulnerability on their own.	4.7	More Details
CVE-2026-122235	Jan from 0.8.5 before 0.8.8 contains a workspace guard bypass vulnerability in the agent-tools gate.rs that allows attackers to write files outside the workspace via dangling symlinks. Attackers supplying a malicious repository can use prompt injection to make the write or edit tools follow symlinks, creating files like ~/.ssh/authorized_keys on the host.	4.7	More Details
	Hisense VIDAA Smart TV firmware V0000.01.00a.P0220 contains an input validation vulnerability in the		

CVE-2026-123995	UPnP/DLNA AVTransport SOAP service that allows a LAN-adjacent attacker to inject arbitrary URIs via the CurrentURI field of SetAVTransportURI without validating the scheme, host, or media legitimacy. Attackers can supply schemes such as http://, file:///data/misc/wifi/, rtsp://, or smb:// to have the TV fetch and render attacker-controlled content after a one-time DLNA pairing, enabling phishing pages, fake firmware prompts, and fake emergency alerts to be displayed, with subsequent commands executing silently.	4.6	More Details
CVE-2026-123996	Hisense VIDAA Smart TV firmware V0000.01.00a.P0220 contains a missing authentication vulnerability in the UPnP/DLNA RenderingControl service on TCP port 38400 that allows a LAN-adjacent attacker to issue SetVolume, SetMute, and SelectPreset(FactoryDefaults) commands after a one-time DLNA pairing with no per-command authentication or session token. Attackers can send a continuous loop of unauthenticated commands to override the physical remote, change volume and mute, and reset all picture and audio calibration settings.	4.6	More Details
CVE-2026-108536	IBM Db2 Genius Hub 1.1.2, 1.1.3, 1.1.4, 1.1.5 could allow a remote authenticated attacker to bypass security restrictions due to improper restriction of rendered UI layers or frames.	4.6	More Details
CVE-2026-122136	Powerlevel10k before 1.20.19 contains a symlink following vulnerability in _p9k_dump_instant_prompt that allows local attackers to overwrite victim-writable files via a predictable temporary path. Attackers can pre-plant symlinks at p10k-instant-prompt-output-<user>-<pid> in TMPDIR, guessing the victim's shell PID, so shell startup truncates and overwrites targeted files.	4.4	More Details
CVE-2026-102703	[This CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] A common access pattern is a batch of Grant Copy operations acting on adjacent address ranges in the same source or destination page. For performance reasons, Xen caches details internally to reuse already validated data. The conditions on when to re-validate the internal data were not correct in some cases: - Frame numbers and grant references could wrongly be mixed up. This is CVE-2026-102703. - Copying by frame number (rather than grant reference) is permitted only when operating on the caller's own memory. The check to enforce this restriction was misplaced. This is CVE-2026-102704.	4.4	More Details
CVE-2026-62855	FreeScout is a self-hosted help desk and shared mailbox. Prior to 1.8.225, the administrator-only App Logs viewer accepts Laravel-encrypted folder and file parameters whose constructed path is checked only as a raw string. An administrator who also knows the APP_KEY can supply traversal segments that the filesystem normalizes outside storage/logs. The /app-logs/app route can then read local files accessible to the PHP worker, including environment files, source files, credentials, tokens, and operating-system files. This issue is fixed in version 1.8.225.	4.4	More Details
CVE-2026-123876	A flaw was found in the default seccomp profile used by Podman via containers-common. Deny rules for AF_VSOCK and NETLINK_AUDIT compared socket arguments with unmasked 64-bit equality. Because the kernel truncates those int arguments to 32 bits, setting upper bits can bypass the deny rules.	4.4	More Details
CVE-2026-100407	Git for Windows is the Windows port of Git. From 2.44.0.windows.1 until 2.55.0.windows.3, the git-credential-wincred store operation in contrib/credential/wincred/git-credential-wincred.c uses _scwprintf() to size a formatted wide-character credential buffer without space for the terminating NUL when both password and oauth_refresh_token are present. The operation also passes a byte count to _snwprintf_s() where a wide-character count is required, allowing the terminator to be written one WCHAR past the heap allocation before CredWriteW() persists the credential. The resulting fixed two-byte NUL overwrite can terminate the helper with Windows heap-corruption status and can cause git credential approve to report success even though the OAuth credential was not stored. This issue is fixed in version 2.55.0.windows.3.	4.4	More Details
CVE-2026-102704	[This CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] A common access pattern is a batch of Grant Copy operations acting on adjacent address ranges in the same source or destination page. For performance reasons, Xen caches details internally to reuse already validated data. The conditions on when to re-validate the internal data were not correct in some cases: - Frame numbers and grant references could wrongly be mixed up. This is CVE-2026-102703. - Copying by frame number (rather than grant reference) is permitted only when operating on the caller's own memory. The check to enforce this restriction was misplaced. This is CVE-2026-102704.	4.4	More Details
CVE-2026-100408	Git for Windows is the Windows port of Git. From 2.43.0.windows.1 until 2.55.0.windows.3, when a matching git:* credential exists in Windows Credential Manager and a git-credential-wincred erase input includes a password field, the operation in contrib/credential/wincred/git-credential-wincred.c allocates a buffer of exactly CredentialBlobSize bytes in match_cred_password() and then uses wcsncpy_s() to copy the corresponding number of wide characters plus a terminating NUL. The destination capacity is also supplied in bytes instead of WCHAR elements, allowing a fixed two-byte NUL write past the allocation before the password comparison determines whether CredDeleteW() should remove the credential; erase without a password field does not enter this comparison path. The helper can terminate with Windows heap-corruption status, and git credential reject can appear successful while the rejected credential remains stored. This issue is fixed in version 2.55.0.windows.3.	4.4	More Details
CVE-2026-123858	In JetBrains PhpStorm before 2026.3 project files could be automatically uploaded to a deployment server from untrusted projects	4.4	More Details
CVE-2026-123782	ChatWiki before 2.10.0 contains an insecure direct object reference vulnerability in SaveFormField and UpdateFormRequired that allows authenticated users to modify other tenants' form fields. Attackers can pass their own form_id to satisfy the ownership check alongside another tenant's sequential form_field id to alter field	4.3	More Details

	names, descriptions, types and required flags, disrupting how submitted entries are stored.		
CVE-2026-122020	A security flaw has been discovered in NST Labs Tech Nstbrowser up to 1.2.1. The affected element is the function stopAllBrowsers of the file /api/agent/browser/stopAll of the component Local Agent Management Service. Performing a manipulation results in denial of service. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-123677	A vulnerability was found in xxyopen/201206030 novel up to 3.5.0. Affected is the function getBookChapter of the file src/main/java/io/github/xxyopen/novel/service/impl/BookServiceImpl.java of the component Book Chapter Read Handler. Performing a manipulation of the argument chapterId results in authorization bypass. The attack may be initiated remotely. The exploit has been made public and could be used. The patch is named b8134e774820e0971fa9d8074405b49a01c99bdc. It is suggested to install a patch to address this issue.	4.3	More Details
CVE-2026-115740	Server side request forgery vulnerability exists in the DLP on-prem extensions version 11.13.1 and earlier allows the file Prefix parameter in the OpenEventEvidenceFile.do endpoint accepts arbitrary UNC paths without validation. The server-side code attempts to open the specified file path, causing Windows to resolve the hostname and initiate SMB authentication to the attacker-controlled host.	4.3	More Details
CVE-2026-122668	Missing Authorization vulnerability in myCred myCred mycred allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects myCred: from n/a through 4.0.2.	4.3	More Details
CVE-2026-122028	A vulnerability has been found in NST Labs Tech Nstbrowser 1.21.0. Affected by this vulnerability is an unknown functionality of the file /agent/info of the component Local Agent API. Such manipulation leads to information disclosure. 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.	4.3	More Details
CVE-2026-120847	Missing Authorization vulnerability in Wpmet Metform metform allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Metform: from n/a through 4.3.3.	4.3	More Details
CVE-2026-122317	SplitPro through 2.1.6 contains an authorization bypass vulnerability that allows authenticated users to retrieve any account's details by supplying arbitrary userId values to user.getUserDetails. Attackers can iterate sequential integer user ids to harvest every user's email, name, avatar, currency, and bankingId and obapiProviderId open-banking identifiers.	4.3	More Details
CVE-2026-123204	Posta before v0.18.0 contains a server-side request forgery vulnerability that allows authenticated users with edit rights to make the backend send POST requests to internal destinations by creating webhooks with arbitrary URLs. Attackers can target loopback, private-network or cloud metadata addresses and read delivery status codes and error strings to probe internal hosts and ports.	4.3	More Details
CVE-2026-123787	A weakness has been identified in nexmoe VidBee up to 1.3.13/2.0.2. The affected element is an unknown function of the file apps/desktop/src/main/local-api.ts of the component Local HTTP Service. Executing a manipulation can lead to information disclosure. The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks. Upgrading to version 2.2.0 is sufficient to fix this issue. This patch is called 141b8d39c1c11da4589264f814cee077df81e7f6. It is suggested to upgrade the affected component.	4.3	More Details
CVE-2026-105191	The ERP: Complete HR, Accounting & CRM Suite Built for WooCommerce WordPress plugin before 1.17.11 does not perform a capability check on an AJAX action that returns the stored before-and-after values of a record change, allowing any authenticated user, including Subscribers, to read other users' sensitive HR, CRM and Accounting data by enumerating record identifiers.	4.3	More Details
CVE-2026-123964	A vulnerability was detected in OpenBMB Internet of Agents up to 9d78e88e47160eb42ee1ee8538c05e1c2c47877a. This affects the function launch_goal of the file im_client/communication/communication_layer.py of the component Collaboration Layer. Performing a manipulation of the argument max_turns results in infinite loop. The attack may be initiated remotely. The exploit is now public and may be used. This product uses a rolling release model to deliver continuous updates. As a result, specific version information for affected or updated releases is not available. The project was informed of the problem early through an issue report but has not responded yet.	4.3	More Details
CVE-2026-120837	Missing Authorization vulnerability in Everest Forms Everest Forms everest-forms allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Everest Forms: from n/a through 3.6.3.	4.3	More Details
CVE-2026-122113	A vulnerability in Realtek's RtUsbA64.sys USB audio driver allows a physically present attacker using a maliciously crafted USB device to trigger unbounded recursion in the driver's topology-parsing logic during device enumeration. Processing the crafted descriptor exhausts the kernel stack and causes a system crash (bugcheck), resulting in a denial of service. No authenticated user session is required.	4.3	More Details
CVE-2026-121724	Missing Authorization vulnerability in WebberZone Contextual Related Posts contextual-related-posts allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Contextual Related Posts: from n/a through 4.5.3.	4.3	More Details

CVE-2026-123468	Missing Authorization vulnerability in StylemixThemes Motors motors-car-dealership-classified-listings allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Motors: from n/a through 1.4.128.	4.3	More Details
CVE-2026-122327	Meelo through 3.13.1 contains a missing authorization vulnerability that allows authenticated non-admin users to modify shared catalog data because RolesGuard does not require Admin on song, track and video write routes. Attackers can send PUT requests to /songs/:idOrSlug, /tracks/:idOrSlug or /videos/:idOrSlug, or POST to /songs/:idOrSlug/merge, to alter genres, reassign tracks and merge songs.	4.3	More Details
CVE-2026-121993	wePOS (Point Of Sale for WooCommerce) before 2.0.3 contains a missing authorization vulnerability in the wepos/v1/payment/process REST route that allows authenticated vendor-level users to mark arbitrary orders as paid and completed by supplying another order's ID. Attackers with only the publish_shop_orders capability (such as Dokan vendor staff) can invoke the payment processing endpoint with an order ID they do not own to trigger the order completion lifecycle, including stock reduction and granting of paid-order access, without making any real payment.	4.3	More Details
CVE-2026-119745	Sender plugin for WordPress before 2.11.3 contains a missing authorization vulnerability that allows any authenticated user, including Subscribers, to access a sensitive diagnostic dump by requesting the admin_post_sender_debug_download action handled by downloadDebugFile() without any capability, nonce, or referer check. Attackers can exploit this flaw via wp-admin/admin-post.php?action=sender_debug_download to retrieve WordPress, PHP, WooCommerce, and server version details, the full active plugin inventory, active theme information, and plugin settings including the connected Sender account resource key and account metadata.	4.3	More Details
CVE-2026-123470	Missing Authorization vulnerability in HivePress HivePress hivepress allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects HivePress: from n/a through 1.8.1.	4.3	More Details
CVE-2026-103019	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to 8.3.0, userSessionLogout() in src/RestControllers/AuthorizationController.php uses decodeToken() to process an id_token_hint without verifying its signature and, when the referenced trusted session is absent, redirects to the caller-supplied post_logout_redirect_uri before validating it against the client's registered redirect URIs. An unauthenticated attacker can craft a logout link that sends a user to an arbitrary external site and invalidates the user's session, enabling convincing phishing flows from the legitimate logout endpoint. The endpoint is reachable when the OpenEMR REST API is enabled. This issue is fixed in version 8.3.0.	4.3	More Details
CVE-2026-124025	Faveo Helpdesk through 2.0.3 contains a broken access control vulnerability in TicketController::ticket_print and the pdfThread endpoint that fails to verify ticket department or assignment. Authenticated agents can request arbitrary ticket ids via GET /ticket/print/{id} to render PDFs of other departments' tickets, including full conversation threads.	4.3	More Details
CVE-2026-124026	Bar Assistant 6.0.0-rc1 before 6.11.0 contains an incorrect authorization vulnerability in CocktailController::copy that allows registered users to bypass source cocktail membership checks. Attackers owning a bar can POST to /api/cocktails/{id}/copy with other bars' cocktail ids to copy private recipes and images into their own bar.	4.3	More Details
CVE-2026-122116	Certain Yealink terminal devices before 2026-04-21 contain an improper access control vulnerability in the Wi-Fi 802.1X PEAP network configuration function. This flaw exposes deployed 802.1X network access authentication credentials to unauthorized users. The latest Yealink firmware has addressed this vulnerability by restricting 802.1X configuration modification privileges to administrator accounts only by default.	4.3	More Details
CVE-2026-119525	Missing Authorization vulnerability in WP Desk Dropshipping XML for WooCommerce dropshipping-xml-for-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Dropshipping XML for WooCommerce: from n/a through 1.7.4.	4.3	More Details
CVE-2026-123748	A security flaw has been discovered in chenyme grok2api up to 3.1.6. Affected by this vulnerability is the function proxyVoiceWebSocket of the file backend/internal/transport/http/inference/voice_ws_handler.go of the component WebSocket Proxy. The manipulation results in resource consumption. The attack may be launched remotely. Upgrading to version 3.1.7 addresses this issue. The patch is identified as 7ad0f791f0a9eb5a0ddfe38ac4dfcef01e19a6d4. It is suggested to upgrade the affected component.	4.3	More Details
CVE-2026-119492	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Metaphor Creations, LLC Ditty ditty-news-ticker allows Code Injection.This issue affects Ditty: from n/a through 3.1.71.	4.3	More Details
CVE-2026-119478	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in StylemixThemes MasterStudy LMS masterstudy-lms-learning-management-system allows Code Injection.This issue affects MasterStudy LMS: from n/a through 3.7.56.	4.3	More Details
CVE-2026-18159	A vulnerability in OpenText OpenText Directory Services (OTDS) on Windows and Linux allows Clickjacking. This issue affects OpenText Directory Services (OTDS): from 10.5 through 26.2.	4.3	More Details
CVE-2026-105702	IBM Db2 Genius Hub 1.1.2, 1.1.3, 1.1.4, 1.1.5 could allow a remote authenticated attacker to obtain sensitive information due to exposure of error messages containing internal implementation details.	4.3	More Details

CVE-2026-62851	FreeScout is a self-hosted help desk and shared mailbox. Prior to 1.8.226, the search-by-number shortcut in ConversationsController::search() resolves a user-controlled ticket number without applying the mailbox filter or view policy used by the normal search path. An authenticated non-admin agent who is a member of at least one mailbox can request /search with a hash-prefixed ticket number and use the 302 Location header to confirm that a conversation exists in a different mailbox the agent cannot access and learn its internal conversation and folder identifiers. The destination conversation remains protected, so this issue does not disclose message content, attachments, or customer data. This issue is fixed in version 1.8.226.	4.3	More Details
CVE-2026-120840	Missing Authorization vulnerability in ThemeGrill User Registration user-registration allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects User Registration: from n/a through 5.3.0.	4.3	More Details
CVE-2026-123857	In JetBrains PhpStorm before 2026.3 xXE was possible in untrusted projects via PHPMD ruleset autodetection	4.3	More Details
CVE-2026-108767	IBM Db2 Genius Hub 1.1.2, 1.1.3, 1.1.4, 1.1.5 could allow a remote authenticated attacker to conduct HTTP response splitting due to improper neutralization of HTTP headers.	4.3	More Details
CVE-2026-118517	The Symfony HtmlSanitizer component UrlSanitizer parses URLs differently from browsers, allowing the allowLinkHosts() and allowMediaHosts() checks to be bypassed for URLs without a well-formed authority, resulting in untrusted hosts being referenced in sanitized output in Symfony versions 6.1.x prior to 6.4.50, 7.x prior to 7.4.23, and 8.x prior to 8.1.11. UrlSanitizer parses URLs with league/uri, which follows RFC 3986, while browsers follow the WHATWG URL standard. For URLs without a well-formed authority, such as http:evil.example, ///evil.example, or https://://evil.example/ the sanitizer finds no host, whereas browsers resolve them to evil.example. The guard added for CVE-2026-45066 missed the zero-slash form, and the host 0 was also skipped because PHP treats it as falsy. This is exploitable when a host allow-list is combined with allowRelativeLinks(true) or allowRelativeMedias(true). The default configuration is not affected.	4.3	More Details
CVE-2026-108910	IBM Db2 Genius Hub 1.1.2, 1.1.3, 1.1.4, 1.1.5 could allow a remote authenticated attacker to obtain sensitive information due to missing required cryptographic step.	4.3	More Details
CVE-2026-110283	IBM Db2 Genius Hub 1.1.2, 1.1.3, 1.1.4, 1.1.5 could allow a remote authenticated attacker to cause a denial of service due to improper validation of user-influenced resource identifiers.	4.3	More Details
CVE-2026-104867	Immich is a high-performance self-hosted photo and video management solution. From 3.0.0 until 3.2.0, the GET /api/admin/users/{id}/calendar-heatmap route in server/src/controllers/user-admin.controller.ts uses the ordinary Permission.UserRead permission without an admin-route requirement, and UserAdminService.getCalendarHeatmap in server/src/services/user-admin.service.ts does not compare the authenticated user with the requested user identifier or perform a separate access check. Any authenticated non-admin user can therefore request another account's upload or capture-date activity heatmap for an arbitrary date range. AssetRepository.getCalendarHeatmap in server/src/repositories/asset.repository.ts filters by owner, date, and deletion state but not visibility, so the returned daily counts and total count include archived and locked assets. The route exposes counts and activity dates but does not return asset metadata or content, and it does not affect integrity or availability. This issue is fixed in version 3.2.0.	4.3	More Details
CVE-2026-61990	Missing Authorization vulnerability in WC Lovers WCFM Membership wc-multivendor-membership allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WCFM Membership: from n/a through 2.12.0.	4.3	More Details
CVE-2026-123846	In JetBrains IntelliJ IDEA before 2026.3 blind SSRF was possible via remote references in JSON Schema validation	4.3	More Details
CVE-2026-17143	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to perform HTML injection due to improper neutralization of user-supplied input.	4.3	More Details
CVE-2026-16679	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote attacker to view arbitrary files on the system due to a path traversal vulnerability. A specially crafted URL request could allow directories outside the intended location to be accessed.	4.3	More Details
CVE-2026-90966	The Essential Real Estate WordPress plugin before 5.3.5 does not verify, in one of its AJAX actions, that a listing package selected for free activation is genuinely free or that the requesting user is entitled to it, allowing a self-registered customer to activate a paid package without payment and cause the site to record a paid invoice at the package's full price.	4.3	More Details
CVE-2026-119800	Ryot is a self-hosted personal tracking application. Prior to 10.5.6, the collectionContents GraphQL query implemented by collection_contents() in crates/services/collection/src/content_operations.rs accepts a caller-controlled CollectionContentsInput.collection_id and returns a collection without checking whether the authenticated user owns it, collaborates on it, or may view it. The caller's user id is used only to annotate the response, allowing any authenticated user who obtains another collection's id to read the owner's identity,	4.3	More Details

	collection name and description, reviews, and complete item list across the tenant boundary. This issue is fixed in version 10.5.6.		
CVE-2026-120849	Missing Authorization vulnerability in WC Lovers WCFM Marketplace wc-multivendor-marketplace allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WCFM Marketplace: from n/a through 3.8.3.	4.3	More Details
CVE-2026-121761	Missing Authorization vulnerability in Infomaniak Network VOD Infomaniak vod-infomaniak allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects VOD Infomaniak: from n/a through 1.5.15.	4.3	More Details
CVE-2026-119473	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in properfraction ProfilePress wp-user-avatar allows Code Injection.This issue affects ProfilePress: from n/a through 4.17.7.	4.3	More Details
CVE-2026-118528	The Directorist: AI-Powered Business Directory, Listings & Classified Ads WordPress plugin before 8.11 does not validate that the requesting user owns the referenced listing before returning its metadata via an AJAX action, allowing authenticated attackers with Subscriber-level access and above to disclose another user's private and unpublished draft listing details, including contact information.	4.3	More Details
CVE-2026-117588	The WP Google Review Slider WordPress plugin before 18.11 does not perform nonce validation when updating its active Google Places configuration, allowing attackers to alter or destroy that configuration via a forged request, provided they can trick a site administrator into following a crafted link.	4.3	More Details
CVE-2026-17215	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to verbose error messages. Error responses contain more information about the system than necessary, which could help an attacker learn about the environment.	4.3	More Details
CVE-2026-82902	Server-Side Request Forgery in ViewDataFile in Apache OFBiz 24.09 before 24.09.08 on all platforms allows a remote authenticated attacker holding only the base webtools permissions (OFBTOOLS_VIEW, WEBTOOLS_VIEW) to cause the server to issue arbitrary outbound HTTP requests, and an attacker additionally holding ENTITY_MAINT and DATAFILE_MAINT to read arbitrary local files via a file: URL, by supplying the DEFINITION_LOCATION or DATAFILE_LOCATION request parameter to the viewdatafile screen, because ViewDataFile.groovy dereferences both parameters as java.net.URL objects with no scheme allow-list, host filter, or egress control inside a screen action that runs before the screen's and template's permission checks are evaluated, so the fetch executes regardless of whether the requesting account is authorized to view its result. Users are recommended to upgrade to version 24.09.08, which fixes this issue.	4.3	More Details
CVE-2026-123467	Missing Authorization vulnerability in StylemixThemes Motors motors-car-dealership-classified-listings allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Motors: from n/a through 1.4.128.	4.3	More Details
CVE-2026-17211	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to cause a denial of service due to incorrect type conversion. A value is converted incorrectly between two different types, which could cause the service to return invalid responses or become unavailable.	4.3	More Details
CVE-2026-123788	A security vulnerability has been detected in chenyme grok2api up to 3.1.6. The impacted element is an unknown function of the file backend/internal/transport/http/inference/voice_ws_handler.go of the component STT Billing. The manipulation leads to enforcement of behavioral workflow. The attack may be initiated remotely. Upgrading to version 3.1.7 is sufficient to resolve this issue. The identifier of the patch is 7ad0f791f0a9eb5a0ddfe38ac4dfcef01e19a6d4. Upgrading the affected component is recommended.	4.3	More Details
CVE-2026-119519	Missing Authorization vulnerability in WProyal Royal Elementor Addons royal-elementor-addons allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Royal Elementor Addons: from n/a through 1.7.1068.	4.3	More Details
CVE-2026-123291	In JetBrains Datalore before 2026.4 improper owner validation allowed reading another workspace's issues and runs notebook	4.3	More Details
CVE-2026-18689	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow an authenticated user to obtain limited information about other organizations due to incorrect authorization. A token issued for a limited purpose is accepted where it should not be, which could reveal the names of other organizations.	4.3	More Details
CVE-2026-123471	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in myCred myCred mycred allows Code Injection.This issue affects myCred: from n/a through 4.0.2.	4.3	More Details
CVE-2026-120851	Missing Authorization vulnerability in PublishPress PublishPress Revisions revisionary allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects PublishPress Revisions: from n/a through 4.2.0.	4.3	More Details
CVE-2026-121585	A security flaw has been discovered in InfiniFlow RAGFlow up to 0.27.2/1.0.0-rc2. This impacts the function RunSQL of the file internal/engine/infinity/sql.go of the component Text To SQL Retrieval. The manipulation of the argument tableName/kbIDs results in authorization bypass. The attack may be performed from remote. The	4.3	More Details

	exploit has been released to the public and may be used for attacks.		
CVE-2026-119486	Missing Authorization vulnerability in WP ManageNinja LLC FluentBoards fluent-boards allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects FluentBoards: from n/a through 2.2.2.	4.3	More Details
CVE-2026-118533	The Directorist: AI-Powered Business Directory, Listings & Classified Ads WordPress plugin before 8.11 does not verify that the user requesting an order's payment receipt owns that order, allowing any authenticated user, such as a subscriber, to disclose other users' order and payment information, including amounts, payment method, payment status and transaction ID.	4.3	More Details
CVE-2026-17144	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to obtain sensitive information due to improper input validation.	4.3	More Details
CVE-2026-122660	Missing Authorization vulnerability in BAKKBONE Australia FloristPress bakkbone-florist-companion allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects FloristPress: from n/a through 7.8.5.	4.3	More Details
CVE-2026-121837	A flaw was found in the REST Data Panache component of Quarkus. When a security constraint is applied to an entity property using the @SecureField annotation on its getter method rather than the field itself, the generated REST resource fails to enforce this constraint for filtering and sorting operations. This allows an authenticated user to infer sensitive data values by observing which records match specific filter criteria or how they are ordered, even though the values are omitted from the final response.	4.3	More Details
CVE-2026-115831	The VOD Infomaniak plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.5.15. 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 initiate unauthorized video imports using the site owner's Infomaniak API credentials, consume the site owner's VOD account quota, and insert arbitrary rows into the wp_vod_upload table causing public shortcodes to resolve to attacker-chosen video content. This action is explicitly reserved for Contributor-level and above by the plugin's own role-rights system, meaning subscriber access is intentionally forbidden by design — the AJAX handler simply omits the enforcement.	4.3	More Details
CVE-2026-90967	The Essential Real Estate WordPress plugin before 5.3.5 does not verify ownership of an invoice before rendering it in one of its AJAX actions, allowing an authenticated low-privileged user to read other users' invoices, including the invoice owner's name, account email address and financial details.	4.3	More Details
CVE-2026-118188	The PublishPress Revisions: Duplicate Posts, Submit, Approve and Schedule Content Changes WordPress plugin before 4.3.1 does not verify that a user is permitted to read a given post before returning its content through its revision-comparison feature, allowing any authenticated user, including a Subscriber, to read the title, content and excerpt of any other user's private, draft, pending, scheduled or trashed post.	4.3	More Details
CVE-2026-119491	Missing Authorization vulnerability in David Lingren Media LIbrary Assistant media-library-assistant allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Media LIbrary Assistant: from n/a through 3.43.	4.3	More Details
CVE-2026-122052	A vulnerability has been found in laspy up to 2.7.0. Affected by this issue is some unknown functionality of the file laspy/lasreader.py of the component LAS File Handler. The manipulation leads to uncontrolled memory allocation. Remote exploitation of the attack is possible.	4.3	More Details
CVE-2026-122144	A security flaw has been discovered in nliautaud pico-content-editor up to 02d5ad6c820c5050c542ab9505819b5e0a0ba1af. This vulnerability affects unknown code. The manipulation results in cross-site request forgery. The attack may be performed from remote. The exploit has been released to the public and may 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 vendor was contacted early about this disclosure but did not respond in any way. This vulnerability only affects products that are no longer supported by the maintainer.	4.3	More Details
CVE-2026-118801	The aBlocks – Gutenberg Blocks, User Dashboard Builder, Popup Builder, Form Builder & Animation Builder plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.18.0 via the 'id' parameter. This makes it possible for authenticated attackers, with contributor-level access and above, to extract the full rendered body content of any password-protected post of any post type by embedding the shortcode with the target post's ID. Author-level attackers and above can additionally publish a post embedding the shortcode, exposing the password-protected content to unauthenticated visitors.	4.3	More Details
CVE-2026-17167	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to falsify audit log information due to reliance on untrusted inputs. Information supplied by the client is relied on when recording the source of a request, so audit records could contain inaccurate details.	4.3	More Details
CVE-2026-122151	A security vulnerability has been detected in Presenton up to 0.9.11-beta. Impacted is the function JSON.parse of the file /api/user-config of the component User Configuration Handler. Such manipulation leads to cross-site request forgery. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used. Upgrading to version 0.9.12-beta is recommended to address this issue. The name of the patch is 44c8a61122b21f17642d717b0c4d6f2c54c0f180. It is recommended to upgrade the affected component.	4.3	More Details

CVE-2026-85570	The Tutor LMS WordPress plugin before 4.2.0 does not prevent the correct answers to quiz questions from being included in the page it serves to the student taking the quiz, and does so regardless of the setting intended to control whether answers are revealed, allowing any enrolled student to obtain them before submitting their attempt.	4.3	More Details
CVE-2026-85346	The FV Flowplayer Video Player WordPress plugin before 7.5.56.7212 does not perform authorization or CSRF checks on several of its cloud storage media browser handlers, allowing any authenticated user with minimal permissions (such as Subscriber) to disclose the configuration and stored file listings of the site's connected cloud storage accounts.	4.3	More Details
CVE-2026-118534	The Directorist: AI-Powered Business Directory, Listings & Classified Ads WordPress plugin before 8.11 does not verify that the order targeted by its checkout payment-retry REST action belongs to the requesting user, allowing any authenticated user, such as a subscriber, to create payment-attempt records against other users' orders.	4.3	More Details
CVE-2026-92080	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in TÜBİTAK BİLGEM Software Technologies Research Institute pardus-boot-repair allows Path Traversal. This issue affects pardus-boot-repair: from 1.0.8 before 1.1.0.	4.3	More Details
CVE-2026-108178	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a token to be accepted that should be rejected due to an improperly implemented security check. Under certain conditions, token validation is incomplete, so a token may be accepted for a purpose it was not intended for.	4.2	More Details
CVE-2026-123011	STMicroelectronics st-mems-android-linux-sensors-hal before 7bdf334 does not check whether the allowed number of channels is exceeded.	4.2	More Details
CVE-2026-96447	A flaw was found in the TokenManager component of Keycloak, an open-source identity and access management solution. The issue occurs during the validation of stateless access tokens when the original user ID no longer exists. Keycloak incorrectly falls back to using the username to identify the user without verifying if the identity matches the original token subject. This could allow an attacker with an old token to gain access to a newly created service account if it shares the same client ID as a previously deleted one.	4.2	More Details
CVE-2026-121857	The Event Tickets with Ticket Scanner WordPress plugin before 3.1.14 does not check that a user may manage WooCommerce orders before returning or removing ticket data for any order, allowing any role an administrator has granted access to the Event Tickets with Ticket Scanner WordPress plugin before 3.1.14's admin area (down to Subscriber) to view other customers' ticket codes and names and to remove tickets from their orders.	4.2	More Details
CVE-2026-124028	mistral.rs before 0.9.5 contains a delimiter injection vulnerability in mistralrs-core that allows attackers to inject tool calls by placing delimiter strings in text the model quotes. Attackers controlling documents, web pages or tool outputs can embed tags like </tool_call> to make qwen-xml, gemma4 or reasoning parsers return extra calls to declared tools with attacker-chosen arguments.	4.2	More Details
CVE-2026-35112	HCL AION is affected by a vulnerability where the Cross-Origin-Embedder-Policy (COEP) header was missing or insecure, so embedded cross-origin resources were not required to explicitly grant permission. This weakens cross-origin isolation, potentially resulting in unintended behavior or security impact under certain conditions.	4.2	More Details
CVE-2026-106128	Prototype Pollution in @progress/kendo-vue-common in Progress Software Kendo UI for Vue versions 0.4.0 through 9.2.0 allows a high-privileged attacker who can control a field path processed by components such as the Scheduler to modify the prototype of built-in objects, resulting in a limited impact on confidentiality, integrity, and availability.	4.1	More Details
CVE-2026-106127	Prototype Pollution in the setter utility (@progress/kendo-react-common) in Progress Software KendoReact versions 3.5.0 through 16.0.0 allows a high-privileged attacker who can control a field path passed to the utility, directly or through components such as the Form, Scheduler, and Gantt, to modify the prototype of built-in objects, resulting in a limited impact on confidentiality, integrity, and availability.	4.1	More Details
CVE-2026-110692	The PowerPack Addons for Elementor: Widgets, Form Styler and Templates WordPress plugin before 3.1.3 does not validate a user-supplied URL before using it in a server-side HTTP request, which could allow users with the contributor role and above to perform Server-Side Request Forgery attacks against internal and loopback resources and read the response back.	4.1	More Details
CVE-2026-106144	Prototype Pollution in the Scheduler component (@progress/kendo-angular-scheduler and @progress/kendo-angular-common) in Progress Software Kendo UI for Angular versions prior to 25.1.0 allows a high-privileged attacker who can control a field path processed by the Scheduler to modify the prototype of built-in objects, resulting in a limited impact on confidentiality, integrity, and availability.	4.1	More Details
CVE-2026-17085	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to bypass security restrictions due to improper handling of case sensitivity. An access restriction is not applied consistently to all variations of the input, which could allow it to be circumvented and unauthorized emails to be sent.	4.1	More Details
CVE-2026-17137	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow a local attacker to obtain sensitive information due to improper use of cryptography. The encryption applied to stored data is not implemented with sufficient strength, which weakens its protection.	4.0	More Details

CVE-2026-19122	IBM API Connect 12.1.0.0 through 12.1.1.2 could allow an authenticated privileged attacker to send unauthorized requests from the system due to server-side request forgery. This could be used to enumerate network resources or to support further attacks.	3.8	More Details
CVE-2026-108068	The FV Flowplayer Video Player WordPress plugin before 7.5.56.7212 does not perform proper authorization checks on one of its video-migration functions, which is protected by a nonce only, allowing users with Contributor-level permissions and above to disclose and bulk-modify the FV Flowplayer Video Player WordPress plugin before 7.5.56.7212's stored video records across the whole site.	3.8	More Details
CVE-2026-108067	The FV Flowplayer Video Player WordPress plugin before 7.5.56.7212 does not properly verify record ownership before modifying or deleting stored video and meta records, allowing authenticated users with Contributor-level access and above to modify or delete arbitrary records belonging to other users, and to disclose the associated meta data in the response.	3.8	More Details
CVE-2026-123333	In JetBrains YouTrack before 2026.2.19562 sprint creation allowed moving issues from inaccessible projects between sprints	3.8	More Details
CVE-2026-123334	In JetBrains YouTrack before 2026.2.19562 project admins of a related project could delete VCS integrations owned by another project	3.8	More Details
CVE-2026-5345	HCL AION is affected by a missing encryption vulnerability in a second WebSocket connection defined in the GenAI web interface. The connection used the unencrypted WebSocket protocol (ws://test) instead of an encrypted (wss://) channel. This may allow data exchanged over the connection to be intercepted or read by an attacker on the network, potentially resulting in unintended behavior or security impact under certain conditions.	3.7	More Details
CVE-2026-121970	Pay with Vipps and MobilePay for WooCommerce (woo-vipps) before 6.4.1 contains an improper cryptographic signature verification vulnerability in the recurring-payment webhook handler that allows unauthenticated attackers to forge webhook requests when no local webhook secret is stored, because the code fails to return on an empty secret and computes an HMAC keyed with an empty string using a loose == comparison instead of hash_equals. Attackers can craft a recurring.agreement-stopped.v1 event with a known agreementId and a matching empty-key signature to cancel a victim's active WooCommerce subscription.	3.7	More Details
CVE-2026-85286	HomeBox is a home inventory and organization system. Prior to 0.27.0, the POST /api/v1/users/login endpoint performs password-hash verification only when the submitted username matches an existing account, while unknown usernames return immediately. Although both paths return the same 401 unauthorized response, the processing-time discrepancy allows an unauthenticated remote attacker to distinguish registered email addresses; rate limiting only reduces the number of attempts per window. This issue is fixed in version 0.27.0.	3.7	More Details
CVE-2026-111962	The WP Remote Users Sync WordPress plugin before 2.2.0 does not adequately restrict access to the user export files it writes beneath the public web root, relying on an Apache access-control file that other web servers such as Nginx ignore, which allows an unauthenticated attacker who requests the export's predictable file name while it is present to retrieve the exported users' personal data.	3.7	More Details
CVE-2026-112337	Wazuh from 3.7.0 before 4.14.9 contains a server-side request forgery vulnerability in the Azure wodle get_graph_events() function that follows @odata.nextLink without host or HTTPS validation. Attackers who influence the nextLink value can redirect manager requests to attacker-controlled endpoints, capturing the reused Microsoft Graph bearer token and reaching internal services.	3.7	More Details
CVE-2026-61813	ModSecurity is an open source, cross platform web application firewall (WAF) engine for Apache, IIS and Nginx. Prior to 2.9.15 and 3.0.17, the HttpsClient::download function in src/utils/https_client.cc sets libcurl CURLOPT_SSL_VERIFYHOST to 1 instead of the strict value 2L. Under adversary-in-the-middle and TLS interception conditions, this non-strict setting may weaken TLS peer identity validation and increase the risk of accepting a certificate for an unintended host. End-to-end exploitation is non-trivial in typical environments. This issue is fixed in versions 2.9.15 and 3.0.17.	3.7	More Details
CVE-2026-122049	A flaw has been found in Campcodes Bitcoin Wallet System 1.0. This affects the function random_int of the file core/app/Http/Controllers/Auth/ForgotPasswordController.php. This manipulation causes improper restriction of excessive authentication attempts. Remote exploitation of the attack is possible. The attack's complexity is rated as high. It is indicated that the exploitability is difficult. The exploit has been published and may be used.	3.7	More Details
CVE-2026-123319	In JetBrains Ktor before 3.6.1 missing Domain attribute validation in client cookie storage allowed cookie injection	3.7	More Details
CVE-2026-88814	The YITH WooCommerce Gift Cards WordPress plugin before 4.38.1 does not lock or atomically update a gift card's balance when it is redeemed at checkout, allowing an attacker who holds a gift card code to spend more than its funded value by submitting multiple checkouts for the same code at the same time.	3.7	More Details
CVE-	The Fluent Support – Helpdesk & Customer Support Ticket System plugin for WordPress is vulnerable to unauthenticated modification of a linked customer's stored profile fields in versions up to, and including, 2.4.7 Its first-party Fluent Forms integration (FeedIntegration::notify()) opens a ticket from each public form submission and, for a logged-out submitter, resolves the submitted email to an existing WordPress account via get_user_by('email', ...) without verifying the submitter controls that address, then passes the attacker-supplied		More

2026-119213	data to Customer::maybeCreateCustomer(). This makes it possible for unauthenticated attackers to overwrite a limited set of a registered customer's stored profile fields where an administrator has enabled a FluentSupport feed on a public form. The email address, role and status are never changed; first and last name are overwritten only when the target user has no name set in user meta; and other fields (title, address, city, state, zip, country) are writable only where an administrator has mapped them in the feed.	3.7	Details
CVE-2026-35114	HCL AION is affected by a vulnerability where the X-Content-Type-Options header was missing or insecure, allowing browsers to MIME-sniff responses. This may cause content to be interpreted as an unintended type, potentially resulting in unintended behavior or security impact under certain conditions.	3.7	More Details
CVE-2026-123206	EdgeChat before 2.20.3 contains a missing authentication vulnerability in the GET /files/:key route that allows unauthenticated or banned users to download decrypted public-channel attachments because canAccessFile() accepts a null user id. Attackers holding an attachment object key can omit or supply an invalid token to retrieve plaintext attachments without a session or channel membership.	3.7	More Details
CVE-2026-35115	HCL AION is affected by a vulnerability where the HTTP Strict-Transport-Security (HSTS) header was missing or insecurely configured, so browsers were not instructed to always use HTTPS. This may allow connections to be downgraded or intercepted, potentially resulting in unintended behavior or security impact under certain conditions.	3.7	More Details
CVE-2026-101166	The Mollie Payments for WooCommerce WordPress plugin before 8.2.0 does not verify a product's publication status before creating an order for it through its PayPal express-checkout endpoint, allowing unauthenticated users to order draft or unpublished products.	3.7	More Details
CVE-2026-122131	Joi 17.13.6 before 17.13.9 and 18.2.5 before 18.3.1 contains a prototype pollution vulnerability in lib/messages.js compile() and merge() that fails to reject a __proto__ language key. Attackers supplying untrusted message configuration via any().messages(), prefs, validate options or Joi.extend can replace the compiled messages prototype, altering or breaking validation error rendering and dependent logic.	3.7	More Details
CVE-2026-118403	The Premium Packages WordPress plugin before 7.3.1 does not verify that the requester owns a guest order before returning its details, allowing unauthenticated visitors who know a guest order's identifier to view its order status, payment status and total.	3.7	More Details
CVE-2026-21849	HCL AION is affected by a missing encryption vulnerability in the WebSocket connection set up by the GenAI web interface. The connection used the unencrypted WebSocket protocol (ws://localhost:8000) instead of an encrypted (wss://) channel. This may allow data exchanged over the connection to be intercepted or read by an attacker on the network, potentially resulting in unintended behavior or security impact under certain conditions.	3.7	More Details
CVE-2026-101165	The Mollie Payments for WooCommerce WordPress plugin before 8.2.0 does not verify an order's payment state or the requested payment gateway before removing a configured payment-surcharge fee, allowing unauthenticated users to reduce an order's total before completing payment.	3.7	More Details
CVE-2026-35109	HCL AION is affected by a vulnerability where pages served over HTTPS could be cached by the browser or intermediate proxies. Sensitive information in cached responses may be retrieved by an unauthorized user with access to the cache, potentially resulting in unintended behavior or security impact under certain conditions.	3.7	More Details
CVE-2026-91163	Warpgate is an open source SSH, HTTPS, and MySQL bastion host for Linux. Prior to 0.29.0, the Kubernetes protocol listener uses AcceptAnyClientCert in warpgate-protocol-kubernetes/src/server/client_certs.rs to accept certificates at the TLS layer and defer validation to warpgate-protocol-kubernetes/src/server/auth.rs, where authentication and lookup failures are rendered verbatim in an HTTP 500 response body. The Kubernetes application in warpgate-protocol-kubernetes/src/server/mod.rs lacks the outer request-logging wrapper used by the HTTP protocol, and failures in warpgate-protocol-kubernetes/src/server/handlers.rs can short-circuit before its inner log point. An unauthenticated network client can therefore induce failures and receive ASN.1/DER parser diagnostics or sea_orm database errors without the attempt being recorded in the gateway log. The disclosed information is limited to internal diagnostics, and no user-data, integrity, or availability impact is established. This issue is fixed in version 0.29.0.	3.7	More Details
CVE-2026-122233	FrankenPHP before 1.13.4 contains an information disclosure vulnerability in worker mode that fails to clear last HTTP stream response headers between requests, because the reset only happens in RSHUTDOWN, which worker requests skip. Later requests calling http_get_last_response_headers() can read headers fetched by earlier requests on the same worker thread, exposing other users' Set-Cookie or token headers from backend APIs.	3.7	More Details
CVE-2026-121748	Node Version Manager (nvm) is a POSIX-compliant shell function for managing multiple node.js versions. In versions 0.27.0 through 0.40.8, when a project's `.npmrc` sets `prefix`, `nvm use` tells the user to run `nvm use --delete-prefix`, which runs `npm config delete prefix` and `npm config delete globalconfig` in the current directory without naming a config file. npm loads the project `.npmrc` before deciding which file to edit, so that file chooses the target: `userconfig=~/.bashrc` makes npm rewrite `~/.bashrc` as ini (corrupting it), and `location=global` with `globalconfig=` leaves the chosen file at mode 0666, which on a shared machine lets another local user write to it. The attacker (the author of a cloned repository or archive, or a local user who can write a shared parent directory) chooses the file but not the bytes written, and no project code runs. Version 0.41.0 no longer lets a project `.npmrc` select which config file `--delete-prefix` edits.	3.6	More Details
CVE-2026-	In JetBrains IntelliJ IDEA before 2026.3 database connections could be established in untrusted projects	3.6	More

123833			Details
CVE-2025-15701	The Easy Social Icons WordPress plugin before 4.0.3 does not sanitise and escape some of its settings before outputting them on front-end pages, which could allow high-privilege users such as Administrators to perform Stored Cross-Site Scripting attacks when the unfiltered_html capability is disallowed, for example on a multisite network.	3.5	More Details
CVE-2026-81816	XML External Entity (XXE) Injection in ContentWorker in Apache OFBiz 24.09 before 24.09.08 on all platforms allows a remote authenticated attacker holding content-author permission to read arbitrary server files and trigger server-side request forgery by storing a crafted text/xml DataResource containing an external entity declaration, causing ContentWorker's rendering of that content — via renderContentAsText and related CMS/help render paths — to parse the stored XML using FreeMarker's default NodeModel.parse DocumentBuilderFactory, which enables neither FEATURE_SECURE_PROCESSING nor external-entity/DTD restrictions, resolving the external entity and returning its content in the rendered response. Users are recommended to upgrade to version 24.09.08, which fixes this issue.	3.5	More Details
CVE-2026-105991	IBM Db2 Genius Hub 1.1.2, 1.1.3, 1.1.4, 1.1.5 could allow a remote authenticated attacker to bypass security restrictions due to a missing Content Security Policy header.	3.5	More Details
CVE-2026-121929	A security flaw has been discovered in EmpireSoft EmpireCMS up to 8.0. Impacted is an unknown function of the file /e/member/mspace/index.php. The manipulation of the argument spacename results in cross site scripting. It is possible to launch the attack 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.	3.5	More Details
CVE-2026-121928	A vulnerability was identified in InfiniFlow RAGFlow up to 0.27.2. This issue affects some unknown processing of the file api/utils/file_utils.py of the component Images API. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The exploit is publicly available and might be used. Upgrading to version 0.27.3 is capable of addressing this issue. The identifier of the patch is 9ea0246f8d453a144fb4f903d163b2ba6b91ed2c. Upgrading the affected component is advised.	3.5	More Details
CVE-2026-123335	In JetBrains YouTrack before 2026.2.19562, 2026.1.14137, 2025.3.169041 missing authorization allowed attaching tags to any issue via the tag issues collection	3.5	More Details
CVE-2026-123268	A security vulnerability has been detected in libyal libvmdk up to 3fdd7839758e9f44ef95e1dfccde8552b860a4fc. Affected is the function libvmdk_extent_table_get_extent_data_file_path of the file libvmdk/libvmdk_extent_table.c of the component Extent Data File Handler. The manipulation leads to memory corruption. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used. This product uses a rolling release model to deliver continuous updates. As a result, specific version information for affected or updated releases is not available. The identifier of the patch is 175d3fc0a0b961f362f16e7560a6169d7213e16b. Applying a patch is the recommended action to fix this issue.	3.5	More Details
CVE-2026-123850	In JetBrains YouTrack before 2026.2.19422 cSS injection was possible in Mermaid diagrams via configuration directives	3.5	More Details
CVE-2026-54373	VitaFit Android application (com.vt.vitafit) before 2.8.1.0 contains a cleartext traffic vulnerability that allows network-based attackers to intercept or modify unencrypted HTTP communications due to the absence of an Android network security configuration. Attackers on an untrusted network can manipulate support content displayed to the user by tampering with unencrypted HTTP traffic between the app and server.	3.5	More Details
CVE-2025-15708	The Live Composer WordPress plugin before 2.1.23 does not sanitise and escape some of its custom post type slug settings before using them in front-end links, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in a multisite setup).	3.5	More Details
CVE-2026-116376	IBM Db2 Genius Hub 1.1.2, 1.1.3, 1.1.4, 1.1.5 could allow a remote authenticated attacker to conduct a phishing attack due to an open redirect vulnerability.	3.4	More Details
CVE-2026-123313	In JetBrains IntelliJ IDEA before 2026.3 improper checks could enable disabled plugins via external dependency settings	3.3	More Details
CVE-2026-123312	In JetBrains IntelliJ IDEA before 2026.3, 2026.2.4 sSRF was possible via annotations.xml files during indexing	3.3	More Details
CVE-2026-19721	Improper restriction of XML external entity reference vulnerability in TÜBİTAK BİLGEM Software Technologies Research Institute İmzager allows Serialized Data External Linking. This issue affects İmzager: from 2.10.5 before 2.10.7.	3.3	More Details
CVE-	Gitleaks through 8.30.1 contains an incorrect permission assignment vulnerability that allows local users to read		

2026-124039	scan reports because cmd/root.go creates the --report-path file with os.Create and default permissions. Unless --redact is passed, other local users on shared hosts or CI runners can read plaintext secrets and matching lines to obtain discovered credentials.	3.3	More Details
CVE-2026-108838	IBM Db2 Genius Hub 1.1.2, 1.1.3, 1.1.4, 1.1.5 could allow a local attacker to cause a denial of service due to uncontrolled resource consumption.	3.3	More Details
CVE-2026-66982	HCL AION is affected by a vulnerability where browser autocomplete was enabled on sensitive login form fields, allowing the browser to store and suggest previously entered values. A malicious user with access to the same browser or system could retrieve saved credentials, potentially resulting in unintended behavior or security impact under certain conditions.	3.3	More Details
CVE-2026-123845	In JetBrains IntelliJ IDEA before 2026.3 path traversal was possible via JSON Schema references in untrusted projects	3.3	More Details
CVE-2026-19731	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in TÜBİTAK BİLGEM Software Technologies Research Institute İmzager allows Path Traversal. This issue affects İmzager: from 2.10.5 before 2.10.7.	3.3	More Details
CVE-2026-90631	Apache OpenOffice documents can contain links. A missing Authorization vulnerability in Apache OpenOffice allowed an attacker to craft a document that would cause external links to be loaded without prompt, possibly transferring the contents of environment variables in the process. This issue affects Apache OpenOffice: through 4.1.16. Users are recommended to upgrade to version 4.1.17, which fixes the issue.	3.3	More Details
CVE-2026-66986	HCL AION is affected by a vulnerability where user sessions did not expire after a sufficient period of inactivity. An unattended authenticated session could be used by another person with access to the same system to view information or perform actions on behalf of the user, potentially resulting in unintended behavior or security impact under certain conditions.	3.3	More Details
CVE-2026-112913	filelock is a platform-independent file lock for Python. From 3.20.4 until 4.2.1, ReadWriteLock and AsyncReadWriteLock on Windows use _connect to attach SQLite to the lock database by pathname, allowing another local account that can create adjacent names to place a database-wal or database-journal side file before acquisition. An undeletable WAL file makes each read or write acquisition fail immediately with sqlite3.OperationalError regardless of timeout. Separately, when the database contains at least one table, a hot journal that grants the lock account modify rights can cause SQLite recovery to delete a file named by that journal only when the lock account has permission to delete the target. The issue requires a directory writable by another account, such as a shared Windows temporary directory, and does not affect private directories. This issue is fixed in version 4.2.1.	3.3	More Details
CVE-2026-123843	In JetBrains IntelliJ IDEA before 2026.3 untrusted projects could trigger changes to GPG agent configuration	3.3	More Details
CVE-2026-121749	Node Version Manager (nvm) is a POSIX-compliant shell function for managing multiple node.js versions. In versions 0.5.0 through 0.40.8, the requested version pattern is passed to `grep` as a bare argument, without `-e`, in `nvm_ls_remote_index_tab`, `nvm_remote_version`, and `nvm_ls_cached`. A `.nvmrc` whose first line starts with `-`, such as `-Rohenpm_[A-Za-z0-9]*`, is parsed as grep options; with GNU grep, `-R` searches the current directory recursively (following symlinks) instead of the version list. On a bare `nvm install`, nvm then treats a matched string from those files as the version, prints it, and requests it from the configured mirror inside download URLs, so for example a repository containing a symlink to `../../.npmrc` can leak the user's npm token to the terminal and to the mirror's and any proxy's logs. The disclosure is read-only and limited to the characters `0-9A-Za-z._+-`. Version 0.41.0 passes every version pattern to grep with `-e`.	3.3	More Details
CVE-2026-123269	A vulnerability was detected in libyal libvmdk. Affected by this vulnerability is the function libvmdk_descriptor_file_read_header of the file libvmdk/libvmdk_descriptor_file.c of the component Descriptor File Parser. The manipulation results in out-of-bounds read. The attack must be initiated from a local position. The exploit is now public and may be used. The patch is identified as 175d3fc0a0b961f362f16e7560a6169d7213e16b. It is best practice to apply a patch to resolve this issue.	3.3	More Details
CVE-2026-17140	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to execute arbitrary code due to improper control of generation of code. Input supplied by a user can influence code generated by the product, which could lead to code execution.	3.3	More Details
CVE-2026-123299	In JetBrains Hub before 2026.2.52519 information disclosure via user search queries was possible	3.1	More Details
CVE-2026-122301	Parse Server before 8.6.114 and 9.0.0 before 9.10.6-alpha.6 returns field values in object create responses to callers that lack read access to the created object through class-level permissions or the object's ACL. An attacker with create permission can create objects to obtain values set by Cloud Code triggers, schema defaults, and the class default ACL.	3.1	More Details

CVE-2026-122325	fossasia eventyay-exhibition through commit f68888e contains an authorization bypass vulnerability in the exhibitor lead creation API that allows exhibitors to access other organizers' attendee data. Exhibitors with lead scanning enabled can submit another event's pseudonymization id or order secret while naming that organizer in the URL to retrieve attendee names, emails, addresses and answers.	3.1	More Details
CVE-2026-122324	SplitPro through 2.1.6 contains an authorization bypass vulnerability that allows authenticated users to read other users' expenses by supplying arbitrary expenseId values to expense.getExpenseDetails. Attackers who obtain an expense UUID, such as removed former participants, can retrieve expense notes, recurrence schedules, and full user rows of participants and group members.	3.1	More Details
CVE-2026-66984	HCL AION is affected by a vulnerability where certain application responses revealed internal server file system paths. This information could help an attacker understand the application structure and plan further attacks, potentially resulting in unintended behavior or security impact under certain conditions.	3.1	More Details
CVE-2026-123207	LibreTV before v2.21.2 contains a server-side request forgery vulnerability that allows authenticated users to bypass checkUpstreamAllowed() by exploiting unpinned DNS resolution in fetchWithSafeRedirects(). Attackers controlling authoritative DNS can return public addresses during validation and internal addresses at connection time via /api/source/test, /api/proxy, /api/search or /api/detail to reach loopback services, private hosts or cloud metadata endpoints.	3.1	More Details
CVE-2026-21834	HCL AION is affected by a vulnerability where the Content-Security-Policy (CSP) security response header was missing from application responses. Without this header, the browser does not restrict the sources of scripts and other content, increasing exposure to cross-site scripting and content-injection attacks, potentially resulting in unintended behavior or security impact under certain conditions.	3.1	More Details
CVE-2026-118529	The Directorist: AI-Powered Business Directory, Listings & Classified Ads WordPress plugin before 8.11 does not verify that a user owns a listing before processing a featured-listing checkout for it, allowing any authenticated user, such as a subscriber, to publish and feature another user's pending listing when the featured listing fee is set to zero.	3.1	More Details
CVE-2026-107787	The CatFolders WordPress plugin before 2.5.7 does not have authorisation checks on a folder maintenance action, allowing users with a role as low as subscriber to reset the per-user ownership of every media folder and disable the CatFolders WordPress plugin before 2.5.7's user restriction setting.	3.1	More Details
CVE-2026-121750	Node Version Manager (nvm) is a POSIX-compliant shell function for managing multiple node.js versions. In versions 0.40.5 through 0.40.8, `nvm_download_artifact` downloads a release archive directly to its final path in `$NVM_DIR/.cache` and verifies its checksum afterwards; on a checksum mismatch it reports an error but leaves the rejected archive in place. A later `nvm install --offline` of the same version installs that cached file without a checksum, so an archive that was just rejected gets installed and its `node` and `npm` run. This gives code execution to a party who can alter the downloaded tarball (for example a poisoned CDN or cache object) but cannot also forge the `SHASUMS256.txt` beside it, if the victim runs `nvm install --offline` for that version after the visible "Checksums do not match" failure and before any online retry. Version 0.41.0 only puts an archive in the cache once its checksum has passed.	3.1	More Details
CVE-2026-123337	In JetBrains YouTrack before 2026.2.19656 users without update permission could change issue visibility	3.1	More Details
CVE-2026-123336	In JetBrains YouTrack before 2026.2.19728 the attachment size limit could be bypassed via AI assistant thread conversion	3.1	More Details
CVE-2026-123314	In JetBrains IntelliJ IDEA before 2026.3, 2026.2.4 xXE attack was possible via an XML response to an HTTP Client request	3.1	More Details
CVE-2026-121937	loonflow before r3.2.3 contains a missing authorization vulnerability in TicketFlowHistoryView that allows any authenticated user to read other users' ticket flow history by supplying a ticket UUID. Attackers can request the ticket_flow_history endpoint, which skips ticket_view_permission_check, to obtain approval comments and processor names, emails and phone numbers.	3.1	More Details
CVE-2026-123320	In JetBrains Toolbox App before 3.9 insufficient warning in the login dialog allowed connecting to a malicious server	3.1	More Details
CVE-2026-121751	Node Version Manager (nvm) is a POSIX-compliant shell function for managing multiple node.js versions. In versions 0.39.6 through 0.40.8, `nvm ls-remote` (and other commands that refresh remote LTS aliases) store the version column of the mirror's `index.tab` in `$NVM_DIR/alias/lts/` without validating it, and `nvm_normalize_lts` later evaluates any suffix of an `lts/-N` value inside shell arithmetic `$((N+1))`. Under bash and zsh, arithmetic evaluation expands command substitutions in array subscripts, so a stored value such as `lts/-10*path[$(cmd)1]` runs `cmd` as the user when the alias is later resolved by purely local commands (`nvm ls`, `nvm alias`, `nvm use --lts`, `nvm which lts/*`), and in every new shell when the `default` alias is `lts/*`. Exploitation requires the victim to use a hostile mirror -- via a compromised mirror or CDN, a network man-in-the-middle of an `http://` mirror, or a maliciously configured `NVM_NODEJS_ORG_MIRROR` -- and to run an affected command. The same sink is also reachable from a project `.nvmrc`, which is treated as hardening. dash is not affected. Version 0.41.0	3.1	More Details

	only passes an all-digit `lts/-N` offset to arithmetic and drops `index.tab` rows whose version is not a valid version string.		
CVE-2026-123665	A weakness has been identified in kubescape up to 4.0.15. Impacted is the function GetWriter of the file core/pkg/resultshandling/printer/printresults.go of the component Output. Executing a manipulation of the argument outputFile can lead to permission issues. The attack requires local access. Upgrading to version 4.0.16 is recommended to address this issue. This patch is called d90f77314c7d4f2b53cf2425844bde2315bd26d2. Upgrading the affected component is advised.	2.8	More Details
CVE-2026-17062	IBM API Connect 10.0.8.0 through 10.0.8.12 and 12.1.0.0 through 12.1.1.2 could allow a remote authenticated attacker to modify internal requests due to improper neutralization of argument delimiters. Special characters in user-supplied input are not handled safely, which could allow additional parameters to be added to a request made by the server.	2.7	More Details
CVE-2026-97191	The Advanced Custom Fields (ACF®) WordPress plugin before 6.8.11 does not re-apply its field-group location rules when persisting values submitted through the post editor save path, allowing users with contributor-level access and above to write custom fields the site restricted to administrators onto their own posts.	2.7	More Details
CVE-2026-97190	The Advanced Custom Fields (ACF®) WordPress plugin before 6.8.11 does not verify that a user is allowed to edit the target object before writing to it during bidirectional relationship synchronization, allowing users with contributor-level access and above to add or remove a reference to their own object on arbitrary posts, users, or terms they cannot otherwise edit.	2.7	More Details
CVE-2026-97189	The Advanced Custom Fields (ACF®) WordPress plugin before 6.8.11 does not perform a read-permission check when it renders and formats the values of its relational fields, allowing users with post-editing access (Contributor and above) to disclose the titles and non-public statuses of other users' unpublished posts.	2.7	More Details
CVE-2026-116472	A security issue was discovered in ingress-nginx where a user with permission to create an Ingress may be able to cause denial of service of the ingress-nginx data plane, or possibly redirect traffic from other Ingresses. Kubernetes clusters are only affected if they are using ingress-nginx. Due to a missing check, the mirror-target Ingress annotation can be used to target an unauthenticated configuration API within the ingress-nginx controller, allowing write commands to be submitted. Corrupting the data within that configuration API results in all traffic through ingress-nginx being dropped until an Ingress configuration change or a controller restart causes the data to be recreated correctly. In principle, this write access could also be used to redirect traffic from other Ingresses controlled by the same ingress-nginx instance. In practice, there is negligible additional risk: such redirection would require privileged information about internal ingress-nginx state, and users can already redirect traffic from other Ingresses controlled by the same ingress-nginx anyway.	2.7	More Details
CVE-2026-118637	The Simple Download Monitor WordPress plugin before 4.1.3 does not properly check the visibility of the content referenced by one of its shortcodes, allowing users with a role as low as Contributor to disclose the title and description of private, draft and other non-public posts.	2.7	More Details
CVE-2026-111740	The Post Duplicator WordPress plugin before 3.0.17 does not check whether the requesting user may view each post before returning a list of posts for a post type, allowing users with a role as low as Contributor to read the titles and hierarchy of other users' draft and private posts.	2.7	More Details
CVE-2026-118187	The PublishPress Revisions: Duplicate Posts, Submit, Approve and Schedule Content Changes WordPress plugin before 4.3.1 does not verify that a user requesting to duplicate or revise a post has access to that specific post, only that they can edit posts of that type, allowing users with contributor-level access and above to duplicate another user's private, draft, pending or scheduled post into one they own and read its full content.	2.7	More Details
CVE-2026-116780	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to 1.11.2, switch_event_expand_headers_check() advanced beyond its heap copy when a positive offset in ${variable:offset} exceeded the variable value's length. The following length calculation and copy appended adjacent heap memory to the expansion result, potentially exposing channel variables, credentials, allocator data, and pointer bytes. The flaw is reachable through configuration templates that slice remote input and through authenticated Event Socket eval or Event Socket expand commands; the separate channel-variable expander used by ordinary dialplan slicing is unaffected. The requester cannot choose adjacent memory and disclosure stops at a zero byte, but repeated expansion can influence the layout. This issue is fixed in version 1.11.2.	2.7	More Details
CVE-2026-107775	The Dokan: AI Powered WooCommerce Multivendor Marketplace Solution WordPress plugin before 5.3.3 does not verify that the acting administrator is authorized to manage each selected user before enabling that user's marketplace seller status, allowing a subsite Administrator on WordPress Multisite to enable selling for users outside their own site, including network-level users they cannot otherwise manage.	2.7	More Details
CVE-2026-123300	In JetBrains Hub before 2026.2.52519 missing authorisation allowed users with read-only access to modify auth module group mappings	2.7	More Details
CVE-2026-123292	In JetBrains Datalore before 2026.4 aPI tokens and sessions of removed or banned users remained valid	2.7	More Details

CVE-2026-71863	SecureDrop is an open-source whistleblower submission system that media organizations can use to securely accept documents from, and communicate with anonymous sources. From 2.13.0 until 2.16.1, running the securedrop-admin install Ansible playbook with journalist alerts disabled leaves the journalist alert key filename empty, causing the copy task to transfer every file in ~/.config/securedrop-admin/, including Onion Service client authentication credentials, to the Monitor Server. An attacker must first compromise the privileged Monitor Server to obtain the credentials, and the credentials remain an additional protection layer rather than sufficient access by themselves because the Journalist Interface still requires a username, passphrase, and MFA, while SSH access still requires SSH keys. This issue is fixed in version 2.16.1.	2.6	More Details
CVE-2026-112907	filelock is a platform-independent file lock for Python. From 3.22.0 until 4.2.1, soft lock classes on Windows read an existing marker with _read_lock_file and remove a stale marker through break_lock_file using pathname operations that wait for an oplock break. Another local account with read access to an unheld marker can keep a Level 1 or batch oplock unanswered, causing SoftFileLock.acquire and related async or fallback locks to wait beyond timeout, blocking=False, and cancel_check. A stale marker under the oplock cannot be broken, but mutual exclusion remains intact and no file other than the marker is accessed. This issue is fixed in version 4.2.1.	2.5	More Details
CVE-2026-121745	Node Version Manager (nvm) is a POSIX-compliant shell function for managing multiple node.js versions. In versions 0.40.0 through 0.40.8, when `NVM_AUTH_HEADER` is set, `nvm_download` passes the credential to curl or wget as a `--header "Authorization: ..."` command-line argument. Process arguments are visible to every local user (on Linux via `ps` or `/proc//cmdline` unless `/proc` is mounted with `hidepid=`; on macOS via `ps`), so another unprivileged account on the same machine can read the token while nvm is downloading during `nvm ls-remote`, `nvm install`, and similar commands, and gain whatever access it grants on the private mirror. Only users who set `NVM_AUTH_HEADER` on a host shared with other local accounts are affected. Version 0.41.0 passes the header to curl on stdin and to GNU Wget in a private temporary config file. BusyBox wget reads no config file, so when it is the only downloader available the header is still passed as an argument.	2.5	More Details
CVE-2026-122190	A vulnerability was found in SourceCodester Online Food Ordering System 1.0. The impacted element is an unknown function of the file admin/add_category.php of the component Category Management. Performing a manipulation of the argument category_title results in cross site scripting. The attack may be initiated remotely. The exploit has been made public and could be used.	2.4	More Details
CVE-2026-85068	Network UPS Tools is a collection of programs which provide a common interface for monitoring and administering UPS, PDU and SCD hardware. From 2.4.2 through 2.8.5, ippon_command in drivers/blazer_usb.c partially initializes char tmp[64] with a short Megatec status query and then passes a fixed eight-byte chunk to usb_control_msg. A malicious firmware-controlled USB device presenting the Mustek Powermust VID 0x06da and Mustek Powermust PID 0x0003 matches blazer_usb_id, selects ippon_subdriver, and can receive the uninitialized trailing stack bytes during normal polling. The disclosure is bounded and read-only, requires physical or supply-chain access to the USB bus, and has no established integrity or availability impact. This issue is scheduled to be fixed in version 2.8.6.	2.4	More Details
CVE-2026-107776	The Dokan WordPress plugin before 5.3.3 does not reconcile the amount credited to a vendor's reverse-withdrawal ledger against the amount actually collected for the payment order, allowing a vendor to clear their outstanding commission debt while paying less than the balance owed when a discount coupon is applied at checkout.	2.2	More Details
CVE-2026-123357	GROBID is machine learning software for extracting information from scholarly documents. Prior to 0.9.1, the Linux non-server PDF conversion path in grobid-core/src/main/java/org/grobid/core/document/DocumentSource.java passes an attacker-influenced PDF filename through DocumentSource.pdfalto, which interpolates the path into a bash -c command string. A single quote in the filename can terminate the intended quoting, and ProcessRunner.run in grobid-core/src/main/java/org/grobid/core/process/ProcessRunner.java starts the resulting command through ProcessBuilder, allowing arbitrary commands to execute with GROBID process privileges. The bundled REST server path is not affected. This issue is fixed in version 0.9.1.	0.0	More Details
CVE-2026-73860	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2026-18107. Reason: This candidate is a duplicate of CVE-2026-18107. Notes: All CVE users should reference CVE-2026-18107 instead of this candidate.	N/A	More Details
CVE-2026-99271	In the Linux kernel, the following vulnerability has been resolved: ALSA: line6: Clear prev_fbuf on capture buffer release A KASAN slab-use-after-free read was reported in submit_audio_out_urb() when generating an impulse test signal: BUG: KASAN: slab-use-after-free in create_impulse_test_signal sound/usb/line6/playback.c:76 [inline] BUG: KASAN: slab-use-after-free in submit_audio_out_urb+0x1848/0x1b20 sound/usb/line6/playback.c:249 Read of size 2 at addr ffff888008d74870 by task syz.2.3214/7785 Allocated by task 11: kmem_cache_alloc_noprof+0x2f0/0x390 mm/slub.c:4144 line6_buffer_acquire+0x1a1/0x220 sound/usb/line6/pcm.c:158 line6_pcm_acquire+0xb6/0x230 sound/usb/line6/pcm.c:329 line6_startup_work+0x3c/0x50 sound/usb/line6/driver.c:728 Freed by task 7785: kfree+0xf8/0x390 mm/slub.c:6566 line6_buffer_release sound/usb/line6/pcm.c:176 [inline] line6_buffer_release+0xa5/0xf0 sound/usb/line6/pcm.c:170 __line6_pcm_release sound/usb/line6/pcm.c:305 [inline] line6_pcm_release+0x5a/0x80 sound/usb/line6/pcm.c:313 snd_toneport_monitor_put+0x11b/0x190 sound/usb/line6/toneport.c:183 line6pcm->prev_fbuf points into the capture PCM stream buffer (line6pcm->in.buffer), which is updated during audio_in_callback() to feed rate synchronization, software monitoring, and impulse test signal generation on playback side. When all capture streams are closed, line6_buffer_release() frees pstr->buffer with kfree(). However, it does not clear line6pcm->prev_fbuf. If playback is subsequently started (e.g. via impulse test signal volume control snd_line6_impulse_volume_put()), submit_audio_out_urb()	N/A	More Details

	dereferences the stale pointer line6pcm->prev_fbuf under in.lock, resulting in a slab-use-after-free read. Clear prev_fbuf and prev_fsize in line6_buffer_release() when releasing the capture stream buffer under in.lock, ensuring that no stale buffer pointer can be accessed by submit_audio_out_urb().		
CVE-2026-48057	Botan is a C++ cryptography library. Prior to 3.13.0, Botan's X.509 Distinguished Name decoder flattens the Attribute-Value Assertions in each Relative Distinguished Name and loses multi-value RDN grouping before DN name-constraint enforcement. An attacker controlling a name-constrained intermediate CA can issue a certificate with a multi-value RDN whose first Common Name matches the permitted constraint and whose second Common Name is attacker-chosen, causing the constraint check to accept the flattened first value. If the certificate contains no subjectAlternativeName extension, the second Common Name can then be accepted as a hostname; Botan does not fall back to Common Name hostname matching when any subjectAlternativeName is present. The exposure is limited to deployments using DN name constraints, which are uncommon outside internal PKIs, and to certificates without a subjectAlternativeName. This issue is fixed in version 3.13.0.	N/A	More Details
CVE-2026-69128	Chartbrew is an open-source web application that can connect directly to databases and APIs and use the data to create charts. In 5.2.2, the AI SQL blocklist omitted sibling PostgreSQL filesystem functions and failed to match double-quoted identifier forms of denied functions. The vulnerable surface is the AI query tool's PostgreSQL SQL-validation blocklist. A team Owner or Admin uses an AI-enabled PostgreSQL connection whose database role can call server-side file functions and causes generated SQL to use an unlisted sibling function or a double-quoted denied function. Unlisted sibling functions remain allowed, and double-quoted function identifiers bypass the denylist regular expressions and reach PostgreSQL. AI features must be enabled and the user must have elevated Chartbrew privileges. A PostgreSQL superuser or pg_read_server_files role can resolve absolute paths to files readable by the PostgreSQL OS user, while a non-superuser is limited to the source-stated PGDATA-relative scope. This vulnerability is fixed in 5.2.3.	N/A	More Details
CVE-2026-107931	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-54589	Chartbrew is an open-source web application that can connect directly to databases and APIs and use the data to create charts. Prior to 5.2.1, the outbound URL guard recognized ordinary IPv4, IPv6, and IPv4-mapped IPv6 destinations but did not recognize IPv4 addresses embedded in NAT64 prefixes. The vulnerable surface is aPI Data Connection outbound requests routed through server/modules/outboundTargetPolicy.js. An authenticated user with permission to create or edit an API connection supplies an attacker-controlled hostname or redirect whose DNS answer is a NAT64 address embedding a private or link-local IPv4 destination. The policy treated the NAT64 address as public; a NAT64 gateway then translated it to the embedded private IPv4 address after validation. The bypass requires a NAT64/DNS64 deployment path and connection-management privileges. IPv4-only deployments are not affected by this specific bypass. The attacker can read responses from 169.254.169.254 cloud metadata and arbitrary internal IPv4 hosts and ports reachable through the NAT64 gateway. This issue is fixed in version 5.2.1.	N/A	More Details
CVE-2026-86005	Chartbrew is an open-source web application that can connect directly to databases and APIs and use the data to create charts. Prior to 5.2.3, the administrative BullMQ dashboard was mounted without an authentication check. The vulnerable surface is the Bull Board/BullMQ administration dashboard at /apps/queues. A remote unauthenticated attacker reaches /apps/queues on a Chartbrew instance where Redis and BullMQ are enabled and a reverse proxy does not independently block the route. The dashboard trusted network reachability as authorization and exposed its queue-management interface directly. Redis and BullMQ must be enabled and the route must be reachable. Available actions depend on the installed Bull Board version and queue state, while confidentiality depends on job payload and log contents. An unauthenticated user can inspect exposed job payloads and logs and, when enabled by the installed version and queue state, retry or delete jobs or otherwise alter queue processing, affecting confidentiality, integrity, or availability. This issue is fixed in version 5.2.3.	N/A	More Details
CVE-2026-71397	Allocation of Resources Without Limits or Throttling vulnerability in elixir-grpc grpc_server allows unauthenticated attackers to exhaust memory and crash the node via an oversized client-streaming or bidirectional-streaming request body. The streaming read clause of 'Elixir.GRPC.Server.Adapters.Cowboy.Handler':info/3 (grpc_server/lib/grpc/server/adapters/cowboy/handler.ex) never checks the configured max_body_size. Only the unary read path enforces that cap. 'Elixir.GRPC.Server.Adapters.Cowboy':reading_stream/1 (grpc_server/lib/grpc/server/adapters/cowboy.ex) appends every received chunk to its buffer until a complete length-prefixed message arrives. A client can declare a very large message and send it across many small HTTP/2 DATA frames, and the server buffers all of it. This issue affects grpc_server: from 1.0.0 before 1.0.6.	N/A	More Details
CVE-2026-55449	CloudBeaver is a cloud database manager. Prior to 26.1.2, its resource-management project resolution accepts project identifiers without validating that they are safe path components. An authenticated user with resource-management privileges can supply a crafted project identifier that causes path resolution to escape the shared-projects directory and enumerate directory names elsewhere on the server. This can disclose filesystem layout information. Arbitrary file reads, writes, and deletion are not confirmed. The issue is fixed in 26.1.2 by validating project names before resolving the shared-project path.	N/A	More Details
CVE-2026-71881	Multiple injection issues in resource metadata fields in GBIF Integrated Publishing Toolkit versions before 3.3.5 allows authenticated remote attackers to execute code in another user's session after user interaction via stored cross-site scripting	N/A	More Details
CVE-	A flaw was found in the Trainer v2 TrainJob API. A user with permissions to create TrainJobs can exploit this by injecting `valueFrom.secretKeyRef` into environment variable definitions. This allows them to read and exfiltrate		More

2026-83495	sensitive information (secrets) from the namespace, leading to a privilege escalation. This occurs when the TrainJob Role-Based Access Control (RBAC) is broader than the Secret read RBAC.	N/A	Details
CVE-2026-63441	2FAuth is a web app to manage Two-Factor Authentication (2FA) accounts and generate their security codes. From 6.1.0 until 8.0.0, App\Services\Traits\ValidatesUrls::isPublicIp() does not recognize the 64:ff9b::/96 and 64:ff9b:1::/48 NAT64 prefixes, so an otpauth URI image parameter can pass an IPv6 literal or DNS64-synthesized address whose embedded IPv4 target is private, link-local, loopback, or cloud metadata. In a deployment with image fetching enabled and a NAT64 translation path to the internal IPv4 target, an account holder can submit the crafted URI directly, or an external attacker can induce a victim to import a crafted URI or migration payload. IconService::buildFromRemoteImage() then issues an HTTP GET to the embedded target, allowing image-shaped responses to be recovered or other endpoints to be probed blindly. This issue is fixed in version 8.0.0.	N/A	More Details
CVE-2026-104267	Botan is a C++ cryptography library. From 2.7.0 until 3.13.0, Botan's Scrypt implementation on 32-bit platforms computes required memory with unchecked multiplication, allowing attacker-controlled Scrypt parameters to wrap the allocation size and create a buffer smaller than the algorithm subsequently writes. The issue affects systems that enable Scrypt and accept arbitrary parameters from a hostile source, including applications that decrypt attacker-supplied encrypted private keys. A triggering parameter set can cause approximately four gigabytes of Scrypt output to be written past the allocated heap buffer, immediately crashing the process and causing denial of service. Arbitrary code execution is not demonstrated and appears difficult, but cannot be excluded from the overwrite primitive. This issue is fixed in version 3.13.0.	N/A	More Details
CVE-2026-99272	In the Linux kernel, the following vulnerability has been resolved: smb: client: validate the data area in SMB2_read() SMB2_read() copies le32_to_cpu(rsp->DataLength) bytes from (char *)rsp + rsp->DataOffset without checking that the range lies within the response actually received. A READ response with DataOffset == 0 makes smb2_get_data_area_len() zero the data length, so smb2_check_message() accepts a frame as short as the fixed response, while SMB2_read() still uses the server-supplied DataLength, capped only by CIFS_MAX_MSGSIZE and the caller's length. A malicious server can answer the synchronous read used by the mfsymlinks (or SFU) symlink parser with an 81-byte READ response carrying DataOffset 0 and DataLength 1067, making the client copy 1067 bytes from a 448-byte receive object (KASAN slab-out-of-bounds; up to 16 KiB in the general case). Clamp a zero (or header-overlapping) DataOffset to read_rsp_size, as handle_read_data() does for the asynchronous path, and reject the response unless DataOffset + DataLength fits within rsp_iov.iov_len. The SMB1 helper was fixed the same way in 5be5bdda5863.	N/A	More Details
CVE-2026-99274	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix fiemap wild read on empty truncated response smb3_fiemap() treats -E2BIG from SMB2_ioctl() as a truncated range blob and loops for the next chunk. If the server reports STATUS_BUFFER_OVERFLOW with OutputCount == 0, SMB2_ioctl() returns -E2BIG with out_data == NULL and out_data_len == 0, and the existing length checks accept the empty result. The loop then evaluates next = out_data[num - 1].file_offset + ... with num == 0, reading 16 bytes before NULL. Reject a truncated range blob that contains no range, so the resume offset is never computed from an empty response. Also require the last range in a truncated blob to advance the resume offset without overflowing, and to stay within the requested range; a malicious or broken server could otherwise make no progress or underflow len and loop forever. Free the previous response buffer before retrying. Reproduced on 6.6.87.2 with a malicious SMB2 server that answers FSCTL_QUERY_ALLOCATED_RANGES with STATUS_BUFFER_OVERFLOW and OutputCount == 0; an FS_IOC_FIEMAP ioctl on the mount oopses in cifs_fiemap() with CR2 = fffffffffffffff8. The code path is unchanged on mainline.	N/A	More Details
CVE-2026-102530	JupyterLab Desktop is the cross-platform desktop application for JupyterLab. Prior to 4.6.2-1, remote-server URLs were inserted into the server-selection dialog and Welcome view without safe encoding. An attacker who convinces a user to submit a crafted URL can execute JavaScript in the Welcome renderer and abuse its privileged IPC bridge to execute arbitrary code with the user’s privileges. The Welcome view also unsafely renders RSS news-feed titles; exploitation through this separate input path requires control over content delivered through the application’s Jupyter Blog feed or its cached feed data, rather than submission of a remote-server URL. This issue affects all supported platforms and is fixed in version 4.6.2-1.	N/A	More Details
CVE-2026-99273	In the Linux kernel, the following vulnerability has been resolved: ksmbd: reserve space for the UTF-16 terminator in stream info smb_strtoUTF16() always writes a terminating zero UTF-16 unit after the converted characters, but get_file_stream_info() budgets only sizeof(struct smb2_file_stream_info) + streamlen * 2 for a stream entry and sizeof(struct smb2_file_stream_info) + 7 * 2 for the trailing "::$DATA" entry. When an entry exactly fills the 448-byte small response buffer, the terminator is written two bytes past the allocation. Reserve one extra UTF-16 unit in both budget checks. The terminator is not part of the wire format, so the reported lengths are unchanged.	N/A	More Details
CVE-2026-114549	NoMachine nxwebrunner Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of NoMachine. Authentication is not required to exploit this vulnerability. The specific flaw exists within the web service, which listens on TCP port 4443 by default. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-30685.	N/A	More Details
CVE-2026-120484	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2026-119167 Reason: This candidate is a reservation duplicate of CVE-2026-119167. Notes: All CVE users should reference CVE-2026-119167 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details

CVE-2019-16490	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-16492	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-16493	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-16494	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-16495	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-16496	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-16497	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-16498	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-16499	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-16500	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-16501	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-16502	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-16503	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-16504	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-16505	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-16506	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-16507	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-7126	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-7856	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details

CVE-2019-7879	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-7883	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-7891	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-7893	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-7907	Rejected reason: Reserved 2019 Magento 1 ID with no published record. Linked to VULN-9633 but never published; left REJECTED after the 2026-11-06 review of wrongly rejected IDs.	N/A	More Details
CVE-2019-16491	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-16489	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-7917	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-16488	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2026-73099	Cross-Site Request Forgery (CSRF) vulnerability in Apache Juneau. The REST server accepts a "content" query parameter that replaces the request body, and this is enabled by default on every HTTP method, including GET. A cross-site link can therefore deliver an attacker-chosen request body to an endpoint without a CORS preflight, defeating protections that rely on the HTTP method or content type instead of an anti-CSRF token. This issue affects Apache Juneau: through 9.2.0. Users are recommended to upgrade to version 9.2.1, which fixes the issue. Applications that do not use the content parameter can also set disableContentParam to true.	N/A	More Details
CVE-2026-73100	Insertion of Sensitive Information into Log File vulnerability in Apache Juneau. The default REST server call logger records request headers for requests that end in a server error, without redacting them. Any client able to cause a server error gets headers such as Authorization, Cookie, Proxy-Authorization and X-API-Key written in cleartext to the application log, exposing them to anyone who can read the logs. This issue affects Apache Juneau: through 9.2.0. Users are recommended to upgrade to version 9.2.1, which fixes the issue.	N/A	More Details
CVE-2026-73101	Generation of Error Message Containing Sensitive Information vulnerability in Apache Juneau. The REST server sends the internal exception class and message to clients in a "Thrown" response header on every error response, and can include internal exception messages in the error body, even when stack-trace rendering is disabled. This reveals implementation details to remote clients. This issue affects Apache Juneau: through 9.2.0. Users are recommended to upgrade to version 9.2.1, which fixes the issue.	N/A	More Details
CVE-2026-73116	Insufficiently Protected Credentials vulnerability in Apache Juneau. The Apache Juneau RestClient followed HTTP redirects while keeping credential headers from the original request, so a server that redirected the client to a different host or port, or from HTTPS to HTTP, could receive headers such as Authorization, Cookie, Proxy-Authorization and X-API-Key. This issue affects Apache Juneau: through 9.2.0. Users are recommended to upgrade to version 9.2.1, which fixes the issue. The fix applies to HTTP clients created by the RestClient builder; applications that supply their own HttpClient must disable automatic redirects or strip credential headers on cross-origin redirects themselves.	N/A	More Details
CVE-2026-73117	Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Response Splitting') vulnerability in Apache Juneau. The Apache Juneau REST server passed response header values and redirect targets to the servlet container unchecked. An application that sets a response header or redirect target from request data could let a remote client inject header lines (where the servlet container does not itself reject CR/LF) or redirect users to an arbitrary external site. The framework itself does not build headers or redirects from request data; exposure depends on application code. This issue affects Apache Juneau: through 9.2.0. Users are recommended to upgrade to version 9.2.1, which fixes the issue. Header values are now sanitized by default; applications that build redirect targets from request data must also switch from sendRedirect() to the new sendSafeRedirect().	N/A	More Details
CVE-	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Apache Juneau. HTML document serialization does not HTML-encode variable substitutions in the page chrome (header,		

2026-96677	nav, aside, footer and similar fields). Applications whose chrome includes request-derived variables, such as request headers, form data or path values, reflect those values unencoded, allowing cross-site scripting. The default chrome does not use request variables, so only applications that add them are affected. This issue affects Apache Juneau: through 9.2.0. Users are recommended to upgrade to version 9.2.1, which fixes the issue.	N/A	More Details
CVE-2026-123119	The Symfony HttpClient component NoPrivateNetworkHttpClient does not pin the checked IP address of cached hosts, allowing for DNS rebinding to bypass private network restrictions, resulting in enumeration of internal hosts and ports in Symfony versions prior to 5.4.56, 6.x prior to 6.4.50, 7.x prior to 7.4.23, and 8.x prior to 8.1.11. NoPrivateNetworkHttpClient resolves the host of each request and checks the IP before connecting. It caches the result per host, and passes the IP to the decorated client through the resolve option so that the client connects to the exact IP that was checked. The issue is that resolve was only passed on the first lookup of a host: on subsequent requests, the decorated client resolved the host again on its own. An attacker who controls a host's DNS can exploit this with DNS rebinding by answering the first lookup with a public IP, and subsequent lookups with a private IP, so when an application sends several requests to that host through the same client, the later requests connect to the private IP. This happens, for example, when an application fetches several URLs of a repository provided by a user. The check of the primary_ip in the on_progress callback still aborts the request before anything is sent, but the connection is made, and the error differs depending on whether the port is open or closed. This allows enumerating internal hosts and ports, as in CVE-2024-50342.	N/A	More Details
CVE-2019-16472	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-16473	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-16474	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-16475	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-16476	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-16477	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-16478	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-16479	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-16480	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-16481	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-16482	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-16483	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-16484	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-16485	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-			

2019-16486	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-16487	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-7916	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-7918	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2026-73095	Allocation of Resources Without Limits or Throttling vulnerability in Apache Juneau. The MessagePack parser, which the REST server enables by default, sizes buffers from length values in the input. An unauthenticated client can send a few bytes that force a multi-gigabyte allocation and an OutOfMemoryError, causing denial of service. Related unbounded allocations in REST request handling (multipart uploads and request reader buffers) are fixed at the same time. This issue affects Apache Juneau: through 9.2.0. Users are recommended to upgrade to version 9.2.1, which fixes the issue.	N/A	More Details
CVE-2020-29089	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29091	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29092	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29093	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29094	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29095	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29096	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29097	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29098	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29099	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29100	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29101	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29102	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-			More

2020-29103	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	Details
CVE-2020-29104	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29105	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29106	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29107	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29108	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29109	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29110	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29111	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29112	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29113	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29090	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29088	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-7920	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29087	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-7922	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-7924	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-7943	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-7949	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-			More

2019-7952	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	Details
CVE-2019-8065	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-8067	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2019-8068	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-24398	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-24399	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-24417	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-24446	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29076	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29077	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29078	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29079	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29080	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29081	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29082	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29083	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29084	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29085	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29086	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
	Improper control of dynamically-loaded code vulnerability in Apache Juneau. When Apache Juneau parses a value		

CVE-2026-73098	into a property of type java.lang.Class (including parameterized forms), the default class swap loaded the named class with initialization enabled, so input naming a class on the application classpath ran that class's static initializer. The impact depends on the classes present in the deployment. This issue affects Apache Juneau: through 9.2.0. Users are recommended to upgrade to version 9.2.1, which fixes the issue.	N/A	More Details
CVE-2026-121489	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Apache Juneau. The microservice DirectoryResource does not keep request paths inside its configured root directory. When an application enables the resource's view, upload or delete settings (all off by default), a client can read, write or delete files outside the root, anywhere the server process has access. This issue affects Apache Juneau: through 9.2.0. Users are recommended to upgrade to version 9.2.1, which fixes the issue.	N/A	More Details
CVE-2026-119217	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate is a reservation duplicate. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2026-110464	Missing authorization in ASUS Armoury Crate allows a local attacker to write content into a specific file or registry location with Local System privileges, or to cause a recoverable system crash, via the service's exposed inter-process interface. Refer to the ' Security Update for Armoury Crate App ' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2026-84729	Out-of-bounds write in certain ASUS Router firmware allow an unauthenticated nearby attacker to write data beyond the intended buffer or potentially cause a denial-of-service (DoS) via a crafted packet. Refer to the ' Security Update for ASUS Router Firmware ' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2026-84730	Stack-based buffer overflow in certain ASUS Router firmware allows an unauthenticated nearby attacker to execute arbitrary commands with root privileges via a crafted device name. Refer to the ' Security Update for ASUS Router AiCloud Feature ' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2026-121803	Rejected reason: This CVE ID is a duplicate of CVE-2026-80335 (VULN-002 dl_download_midst) and has been rejected.	N/A	More Details
CVE-2026-105296	Multiple Akeeba products lack the anti-CSRF check on some actions. If the user access a malicious page while logged into the product, unintended operations may be performed.	N/A	More Details
CVE-2026-11749	A vulnerability has been identified in armeria-saml prior to 1.41.1, where bearer assertions are not enforced for one-time use, allowing replay of previously consumed assertion IDs within their validity period.	N/A	More Details
CVE-2026-11753	A vulnerability has been identified in armeria-saml versions prior to 1.41.1, where attacker-controlled RelayState is reflected into the HTTP Location header after successful authentication, allowing an unvalidated redirect to an attacker-controlled URL.	N/A	More Details
CVE-2026-110944	Resource exhaustion vulnerability in the HTTP request handling of the QHttpServer component of Qt HTTP Server.	N/A	More Details
CVE-2026-114420	SEPPmail Secure Email Gateway before 15.1.1 does not neutralize LDAP metacharacters in an unauthenticated account-selection input in its GINA web interface. A remote unauthenticated attacker can enumerate email addresses.	N/A	More Details
CVE-2026-114421	SEPPmail Secure Email Gateway before 15.1.1 permits password recovery for a created but unregistered GINA account whose initial password is empty without adequately verifying ownership. A remote unauthenticated attacker who identifies such an account can set a new password, authenticate as that account, and prevent the intended recipient from using it until recovery.	N/A	More Details
CVE-2026-114424	SEPPmail Secure Email Gateway before 15.1.1 can evaluate attacker-influenced replacement text as Perl code in sender or recipient replacement rules. An unauthenticated remote sender can execute operating-system commands in the mail-processing worker context when an active rule uses message-derived replacement data and its search condition matches. The validated worker context was root.	N/A	More Details
CVE-2026-114425	SEPPmail Secure Email Gateway before 15.1.1 trusts a file path supplied in externally provided Large File Transfer attachment metadata. An unauthenticated remote sender can cause the mail-processing worker to disclose, move, or delete an accessible regular file when LFT is enabled and the message reaches an affected secure-mail processing path. The validated workers ran as root.	N/A	More Details
CVE-2026-114426	SEPPmail Secure Email Gateway before 15.1.1 processes and writes v1 file-interface upload data before authenticating the caller and without an absolute request-size limit. An unauthenticated remote attacker can occupy workers and consume temporary storage with concurrent or slow requests, causing service unavailability.	N/A	More Details
CVE-2026-	Server-side request forgery (SSRF) vulnerability in the Coupa Supplier Portal SaaS platform, specifically in the document conversion functionality available in the ‘Contracts > Templates’ section. The vulnerability is due to insufficient validation of references to external resources processed by the Aspose.Words for Java library during DOCX-to-PDF conversion. An authenticated attacker with permissions to modify templates could upload a	N/A	More

111036	specially crafted DOCX document containing references to external resources, which would cause the server-side application to access URLs controlled by the attacker, resources on the internal network, or local files. A successful exploit could lead to the disclosure of sensitive information, such as configuration files, system files, credentials, environment variables and endpoints for internal services.		Details
CVE-2026-111037	A reflected Cross-Site Scripting (XSS) vulnerability in the Tenders module of the Coupa Supplier Portal SaaS platform. The vulnerability arises because the `list_item_function` parameter is reflected in the server's response without proper output encoding or sanitisation, and is directly embedded within the context of a JavaScript event handler. An attacker with a low-privileged account could create a malicious URL containing JavaScript payloads which, when opened by a victim, would execute arbitrary scripts within the context of the victim's browser. A successful exploit could allow the attacker to perform actions on the victim's behalf, disclose accessible information or manipulate the user interface.	N/A	More Details
CVE-2026-111038	CSV formula injection vulnerability in the export functionality of the Coupa Supplier Portal SaaS platform. The vulnerability arises because certain user-controlled data, such as event names or templates within the Tenders module, are not properly validated or sanitised before being included in CSV files generated by the application. An attacker with low privileges can input specially crafted values that begin with characters interpreted as formulas by spreadsheet applications. When a victim downloads and opens the generated file in a compatible client, the content may be interpreted as a formula, potentially leading to unauthorised actions such as the execution of commands via mechanisms such as DDE, access to information, or interaction with system resources under the victim's context.	N/A	More Details
CVE-2026-111040	The platform allows persistent HTML injection into editable fields managed by TinyMCE. An authenticated attacker with low privileges can inject unsanitised HTML content which is stored in the database and subsequently rendered in other users' browsers, affecting the display of content within the application.	N/A	More Details
CVE-2026-120422	Sogou Input Method for Windows contains a vulnerability in the configuration retrieval mechanism of its SGTool.exe component. The application retrieves configuration data over unencrypted HTTP connections, allowing an attacker capable of manipulating network traffic to replace legitimate server responses with malicious configurations. An attacker can exploit this vulnerability to instruct SGTool.exe to download attacker-controlled files to arbitrary locations, including paths used by legitimate application components. This can result in arbitrary code execution when the downloaded files are subsequently executed or loaded by the application.	N/A	More Details
CVE-2026-94459	IRISPowerscan contain default user accounts with predictable credentials. An unauthenticated attacker with access to an affected installation could use these credentials to authenticate to the application and access functionality available to the affected accounts, potentially resulting in unauthorised access or modification of application data and configuration.	N/A	More Details
CVE-2026-94460	IRISPowerscan contain an insecure default configuration where the built-in installation account is assigned elevated privileges with a predictable password, which could allow an unauthenticated attacker to gain unauthorised access to privileged application functionality.	N/A	More Details
CVE-2026-95649	IRISPowerscan insufficiently restrict the use of untrusted scripts. An authenticated user with access to script functionality can import or modify scripts that are executed by the application, potentially resulting in arbitrary code execution in the security context of the Windows user running IRISPowerscan.	N/A	More Details
CVE-2026-100235	Incorrect authorization due to a time-of-check to time-of-use (TOCTOU) race condition in the setACL request handling of Apache ZooKeeper. When a node's ACL is changed via setACL, the pending change is not published to the server's outstanding change record for that node. Any request that is prepared (and authorized) after the setACL is submitted but before it commits is therefore checked against the previous, pre-revocation ACL, yet is applied to the data tree after the ACL change has taken effect. A client that currently holds a permission can use this window to perform operations requiring that permission through and after its revocation — for example, committing writes or deletes after losing write access, or re-granting itself full permissions, which persistently defeats the revocation. In deployments transitioning from the default OPEN_ACL_UNSAFE ACL to a restrictive ACL, any unauthenticated client can exploit this during the transition. This issue affects Apache ZooKeeper up to and including 3.9.6. Users are recommended to upgrade to version 3.8.8 or 3.9.7, which fixes the issue.	N/A	More Details
CVE-2026-100252	Improper Authorization vulnerability in Apache ZooKeeper. When SASL authentication is enabled on the client port, the server's SASL callback handler grants every authorization identity (authzid) that a client requests, without checking it against the principal the client authenticated as. The server then tries to replace the requested identity with a canonical form of the authenticated principal, derived from the zookeeper.security.auth_to_local rules. If no rule applies to the principal, canonicalization fails and the error is only logged. The client-requested authzid then becomes the session's SASL identity for all ACL checks. An authenticated client whose principal is not covered by the auth_to_local rules can therefore claim any SASL identity. With the default rules, this includes any Kerberos principal from a realm other than the server's default realm, such as a principal from a cross-realm trusted realm. The client then gets the permissions granted to that identity in sasl ACLs. If the requested identity matches a configured zookeeper.superUser, it gets superuser access to the whole data tree. Users are recommended to upgrade to version 3.8.8 or 3.9.7, which fixes the issue.	N/A	More Details
CVE-2026-100300	Improper handling of exceptional conditions in the quota subsystem of Apache ZooKeeper allows an attacker able to write under the /zookeeper/quota subtree — unauthenticated on default deployments, where that subtree is world-writable — to crash the server's critical request-processing thread and render the on-disk data directory permanently unbootable. This issue affects Apache ZooKeeper up to and including 3.9.6. Users are recommended to upgrade to version 3.8.8 or 3.9.7, which fixes the issue.	N/A	More Details

CVE-2026-112116	An exposed IOCTL with insufficient access control in ASUS System Control Interface allows a local, low-privileged user to read and write arbitrary physical memory through crafted device control requests, ultimately resulting in a complete compromise of the affected system. Refer to the ' Security Update for ASUS System Control Interface ' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2026-92211	Pixar Animation Studio OpenUSD Crate File Parsing Double Free Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Pixar Animation Studio OpenUSD. Interaction with this library is required to exploit this vulnerability but attack vectors may vary depending on the implementation. The specific flaw exists within the parsing of USDC and USDZ files. The issue results from the lack of validating the existence of an object prior to performing further free operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-30428.	N/A	More Details
CVE-2026-108500	Input validation vulnerability in Apache ActiveMQ configured to use the LDAPAuthorizationMapPlugin allows an authenticated attacker to create or address a destination with a crafted name containing LDAP DN special characters (such as comma, plus, equals, backslash) can manipulate the LDAP search base used for ACL lookups. This issue affects Apache ActiveMQ: from 6.3.0 before 6.3.3, from 5.19.0 before 5.19.12. Users are recommended to upgrade to version 6.4.0, 6.3.3 or 5.19.12, which fixes the issue.	N/A	More Details
CVE-2026-92200	Quest Foglight for Databases Incorrect Permission Assignment Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of Quest Foglight for Databases. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the product installer. The issue results from incorrect permissions on a folder used by the product. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-31118.	N/A	More Details
CVE-2026-114551	MailEnable Auth Cleartext Storage Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of MailEnable. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of mailbox credentials. The issue results from storing sensitive information in plaintext. An attacker can leverage this in conjunction with other vulnerabilities to disclose stored credentials, leading to further compromise. Was ZDI-CAN-34478.	N/A	More Details
CVE-2026-114552	MailEnable parseObjectResponse XML External Entity Processing Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of MailEnable. Authentication is required to exploit this vulnerability. The specific flaw exists within the implementation of the parseObjectResponse method. The issue results from the lack of proper restriction of XML External Entity (XXE) references. An attacker can leverage this vulnerability to disclose information in the context of the service account. Was ZDI-CAN-29137.	N/A	More Details
CVE-2026-118623	MLflow PickleEvaluationArtifact Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of MLflow. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of pickle files. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-29513.	N/A	More Details
CVE-2026-118624	MLflow Tracking Server Jobs Missing Authorization Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of MLflow. Authentication is required to exploit this vulnerability. The specific flaw exists within the _find_validator function. The issue results from the lack of authorization prior to allowing access to functionality. An attacker can leverage this vulnerability to disclose information in the context of the service account. Was ZDI-CAN-31894.	N/A	More Details
CVE-2026-118625	MLflow Tracking Server Missing Authorization Privilege Escalation Vulnerability. This vulnerability allows remote attackers to escalate privileges on affected installations of MLflow. Authentication is required to exploit this vulnerability. The specific flaw exists within the get_endpoints function. The issue results from the lack of authorization prior to allowing access to functionality. An attacker can leverage this vulnerability to escalate privileges to resources normally protected from the user. Was ZDI-CAN-32107.	N/A	More Details
CVE-2026-118626	MLflow Tracking Server Issues Missing Authorization Privilege Escalation Vulnerability. This vulnerability allows remote attackers to escalate privileges on affected installations of MLflow. Authentication is required to exploit this vulnerability. The specific flaw exists within the configuration of the BEFORE_REQUEST_HANDLERS. The issue results from the lack of authorization prior to allowing access to functionality. An attacker can leverage this vulnerability to escalate privileges to resources normally protected from the user. Was ZDI-CAN-32108.	N/A	More Details
CVE-2026-118627	MLflow SHAP load_explainer Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of MLflow. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the loading of SHAP explainer models. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-30301.	N/A	More Details
CVE-	MLflow get-artifacts Server-Side Request Forgery Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of MLflow. Authentication is not		More

2026-118628	required to exploit this vulnerability. The specific flaw exists within the get-artifacts function. The issue results from the lack of proper validation of a URI prior to accessing resources. An attacker can leverage this vulnerability to disclose information in the context of the server. Was ZDI-CAN-28192.	N/A	Details
CVE-2026-92185	Quest Foglight for Databases AbstractParser XML External Entity Processing Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of Quest Foglight for Databases. Authentication is not required to exploit this vulnerability. The specific flaw exists within the AbstractParser class. Due to the improper restriction of XML External Entity (XXE) references, a crafted document specifying a URI causes the XML parser to access the URI and embed the contents back into the XML document for further processing. An attacker can leverage this vulnerability to disclose information in the context of SYSTEM. Was ZDI-CAN-28929.	N/A	More Details
CVE-2026-92186	Quest Foglight for Databases paFnUploadFileAndCreateInfo Directory Traversal Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Quest Foglight for Databases. Authentication is required to exploit this vulnerability. The specific flaw exists within the paFnUploadFileAndCreateInfo script. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-29038.	N/A	More Details
CVE-2026-92187	Quest Foglight for Databases extractAndCreateUploadInfoList Directory Traversal Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Quest Foglight for Databases. Authentication is required to exploit this vulnerability. The specific flaw exists within the extractAndCreateUploadInfoList method. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-29039.	N/A	More Details
CVE-2026-92188	Quest Foglight for Databases ForgeMBeanServerSupport Missing Authentication Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Quest Foglight for Databases. Authentication is not required to exploit this vulnerability. The specific flaw exists within the ForgeMBeanServerSupport module. The issue results from the lack of authentication prior to allowing access to functionality. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-29168.	N/A	More Details
CVE-2026-92189	Quest Foglight for Databases writeTopologySectionToFile External Control of File Path Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Quest Foglight for Databases. Authentication is not required to exploit this vulnerability. The specific flaw exists within the writeTopologySectionToFile method. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-29169.	N/A	More Details
CVE-2026-92190	Quest Foglight for Databases baseRmiServiceExporter Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Quest Foglight for Databases. Authentication is not required to exploit this vulnerability. The specific flaw exists within the configuration of the baseRmiServiceExporter bean. The issue results from the lack of proper validation of user-supplied data prior to deserializing it. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-29170.	N/A	More Details
CVE-2026-92191	Quest Foglight for Databases runScript Incorrect Authorization Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Quest Foglight for Databases. Authentication is required to exploit this vulnerability. The specific flaw exists within the runScript function. The issue results from incorrect authorization prior to allowing access to functionality. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-29192.	N/A	More Details
CVE-2026-92192	Quest Foglight for Databases installLicense Directory Traversal Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Quest Foglight for Databases. Authentication is required to exploit this vulnerability. The specific flaw exists within the installLicense script. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-29215.	N/A	More Details
CVE-2026-92193	Quest Foglight for Databases FileServlet External Control of File Path Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of Quest Foglight for Databases. Authentication is required to exploit this vulnerability. The specific flaw exists within the FileServlet class. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to disclose information in the context of SYSTEM. Was ZDI-CAN-29216.	N/A	More Details
CVE-2026-92194	Quest Foglight for Databases loadManageServerLicense Directory Traversal Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Quest Foglight for Databases. Authentication is required to exploit this vulnerability. The specific flaw exists within the loadManageServerLicense script. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-29231.	N/A	More Details

CVE-2026-92195	Quest Foglight for Databases loadEvolveLicense Directory Traversal Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Quest Foglight for Databases. Authentication is required to exploit this vulnerability. The specific flaw exists within the loadEvolveLicense script. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-29232.	N/A	More Details
CVE-2026-92196	Quest Foglight for Databases renderTemplateString Server-Side Template Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Quest Foglight for Databases. Authentication is required to exploit this vulnerability. The specific flaw exists within the renderTemplateString method. The issue results from the lack of proper validation of a user-supplied string before processing it with the template engine. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-29889.	N/A	More Details
CVE-2026-92197	Quest Foglight for Databases unzipFile Directory Traversal Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Quest Foglight for Databases. Authentication is required to exploit this vulnerability. The specific flaw exists within the unzipFile method. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-29901.	N/A	More Details
CVE-2026-92198	Quest Foglight for Databases getSource XML External Entity Processing Information Disclosure Vulnerability. This vulnerability allows remote attackers to initiate arbitrary server-side requests on affected installations of Quest Foglight for Databases. Authentication is not required to exploit this vulnerability. The specific flaw exists within the getSource method. Due to the improper restriction of XML External Entity (XXE) references, a crafted document specifying a URI causes the XML parser to access the URI and embed the contents back into the XML document for further processing. An attacker can leverage this vulnerability to disclose information in the context of the application. Was ZDI-CAN-29934.	N/A	More Details
CVE-2026-92199	Quest Foglight for Databases EncryptionUtil Hardcoded Encyption Key Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of Quest Foglight for Databases. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the symmetricDecrypt method. The issue results from the use of a hard-coded cryptographic key. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-29967.	N/A	More Details
CVE-2026-100302	Allocation of Resources Without Limits or Throttling in the multiRead request handler of Apache ZooKeeper allows a remote attacker to crash the server (denial of service) with a single small request. The multiRead handler places no limit on the number of bundled read operations or on the cumulative size of the response it builds in memory. Because each operation's result is fully materialized and retained before serialization, a request that is small on the wire — within the jute.maxbuffer limit — but that references a large znode many times can force the server to allocate far more heap than the request size implies, exhausting the JVM heap and terminating the server with an OutOfMemoryError. Neither jute.maxbuffer nor largeRequestMaxBytes prevents this, as both bound only the inbound request, not the response. This issue affects Apache ZooKeeper from 3.7.0 through 3.9.6. Users are recommended to upgrade to version 3.9.7, which enforces configurable limits on the multiRead operation count and cumulative response size.	N/A	More Details
CVE-2026-115448	Uncontrolled recursion in Apache ZooKeeper. The server serializes its data tree to a snapshot by recursing one stack frame per znode level, with no depth bound. A client permitted to create znodes (the default root ACL is open) can build a chain of nested znodes deep enough that taking a snapshot exhausts the JVM stack and kills the snapshot thread; sizes stay within jute.maxbuffer, so existing limits do not prevent it. This is a denial of service that becomes persistent: on restart the server rebuilds the deep tree from its transaction log and fails again while taking the startup snapshot, so it does not return to service, and recovery can entail data loss. The same log affects a leader and its followers, so it can spread across an ensemble. This issue affects Apache ZooKeeper 3.8.0 through 3.8.7 and 3.9.0 through 3.9.6. Users are recommended to upgrade to 3.8.8 or 3.9.7, which fix the issue. As a workaround, use ACLs and authentication to restrict znode creation rather than relying on the default open root ACL.	N/A	More Details
CVE-2026-118869	An OS command injection vulnerability exists in SHIRASAGI, which may allow an authenticated attacker to execute arbitrary OS commands on the system running the product.	N/A	More Details
CVE-2026-113373	Sonatype Nexus Repository 3 Pro does not check the local account status when a user signs in through a configured SAML or OAuth2/OpenID Connect identity provider. A user whose account was disabled or locked by an administrator in Nexus Repository can sign in again with valid identity provider credentials for the same account, and then receives a new session with the roles of that account. The attacker needs no Nexus Repository session and no Nexus Repository privilege. The attacker needs a named account that holds valid credentials at the identity provider. The anonymous user is not part of this attack path.	N/A	More Details
CVE-2026-	SumatraPDF is a multi-format reader for Windows. In version 3.6.1 and earlier, HttpGet() in src/base/Http_win.cpp unconditionally passes INTERNET_FLAG_IGNORE_CERT_CN_INVALID to WinINet, disabling hostname matching for HTTPS update metadata and crash-symbol requests while retaining certificate-chain validation. A network-positioned attacker with a Windows-trusted certificate for an attacker-controlled domain can impersonate the	N/A	More

115758	project's update host, inject promo text and a clickable URL before update metadata validation, and provide an attacker-controlled archive to ExtractSymbols(). Installer replacement is not directly possible because HttpGetToFile() validates TLS and MaybeStartUpdateDownload() restricts the download host. No fixed version is available as of this review.		Details
CVE-2026-102280	Sandboxie-Plus is an open source sandbox-based isolation software for Windows. Prior to 1.18.6, a process inside a sandbox could send MSGID_FILE_SET_ATTRIBUTES or MSGID_FILE_SET_SHORT_NAME to SbieSvc and cause the SYSTEM service to open and modify an existing file outside the sandbox. The direct primitive changes file attributes, timestamps, writeability, or 8.3 short names; a short-name redirection can additionally contribute to SYSTEM code execution when a privileged process resolves an attacker-controlled short-name path in a location SbieSvc can open. This vulnerability is fixed in 1.18.6.	N/A	More Details
CVE-2026-54379	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-76893	tsParticles is a TypeScript library for creating highly customizable particle animations. Prior to 4.3.2, the HTTP mode of @tsparticles/mcp-server reuses one stateful StreamableHTTPServerTransport for every client. An unauthenticated client that sends the first initialize request without an mcp-session-id claims the shared transport state, causing later independent clients to receive Server already initialized and preventing them from establishing sessions until the process restarts. The first client's session remains functional. This issue is fixed in version 4.3.2.	N/A	More Details
CVE-2026-102337	Webmin is a web-based system administration tool for Unix-like servers. Prior to 2.652, untrusted users with access to the File Manager or Upload and Download modules can direct Webmin's server-side URL download functionality to non-public network addresses because download destinations are not restricted by resolved IP address. This allows requests to unauthenticated intranet services or cloud-provider instance metadata endpoints that are inaccessible from the user's own system. This issue is fixed in 2.652.	N/A	More Details
CVE-2026-108387	radare2 is a UNIX-like reverse engineering framework and command-line toolset. Prior to 6.2.2, attacker-controlled data from several binary format plugins could reach RBinInfo->bclass. Opening or analyzing a crafted Pebble or Sega Mega Drive binary could place a dbg:// URI in bclass, causing radare2 to reopen the input through the debug input/output plugin and ultimately pass attacker-controlled arguments to execvp(). This could execute commands with the privileges of the radare2 process without an explicit debugging command. This issue is fixed in version 6.2.2.	N/A	More Details
CVE-2026-47678	GLPI is a free asset and IT management software package. From 9.4.0 until 10.0.26 and 11.0.8, any authenticated user can submit crafted values to the dropdown values fetching endpoint that are incorporated into a database query. This permits SQL injection through the dropdown endpoint. This issue is fixed in versions 11.0.8 and 10.0.26.	N/A	More Details
CVE-2026-52848	GLPI is a free asset and IT management software package. From 11.0.0 until 11.0.8, during the login phase, an unauthenticated user could use a crafted URL to skip one-time-password verification, defeating two-factor authentication. This issue is fixed in version 11.0.8.	N/A	More Details
CVE-2026-53631	GLPI is a free asset and IT management software package. From 0.83 until 10.0.27 and from 11.0.0 until 11.0.9, any authenticated user could submit a crafted request to change the visibility of knowledge base items, reminders, or RSS feeds and then access content that should remain restricted. This issue is fixed in versions 10.0.27 and 11.0.9.	N/A	More Details
CVE-2026-57152	GLPI is a free asset and IT management software package. From 0.85 until 10.0.26 and from 11.0.0 until 11.0.8, under certain conditions, GLPI permission logic could grant a user access to a document without confirming that the document was linked to the targeted item. This could expose the file to a user who should not be able to view it. This issue is fixed in versions 10.0.26 and 11.0.8.	N/A	More Details
CVE-2026-62662	Pocket ID is an OIDC provider that allows users to authenticate with their passkeys to services. From 1.11.0 until 2.10.0, createTokenFromClientCredentials in backend/internal/service/oidc_service.go accepts the client-controlled resource parameter and embeds it directly in the access token aud claim without validating that the audience is registered or that the requesting client may access it. Any authenticated OIDC client can therefore obtain a Pocket ID-signed token naming another client or an arbitrary audience. The /api/oidc/introspect endpoint cannot distinguish the unauthorized token because it treats a token as active when the introspecting client's identifier matches the attacker-selected audience. In deployments where resource servers trust Pocket ID access tokens for service-to-service authorization, this bypasses audience-based access controls and can permit unauthorized data access or actions; deployments that do not use these tokens for resource-server authorization have no immediate exploitable impact. This issue is fixed in version 2.10.0.	N/A	More Details
CVE-2026-76826	tsParticles is a TypeScript library for creating highly customizable particle animations. From 4.0.0 until 4.3.2, the stable publish workflow interpolates steps.release.outputs.body directly into an echo command in Bash source before writing RAW_RELEASE.md. Contributor-controlled shell metacharacters in generated release-note text can therefore execute when a maintainer starts a stable release, allowing modification of generated artifacts or workspace scripts and affecting later release steps that hold GITHUB_TOKEN and write permissions. This issue is fixed in version 4.3.2.	N/A	More Details
	tsParticles is a TypeScript library for creating highly customizable particle animations. Prior to 4.3.1, the HTTP		

CVE-2026-76892	mode of @tsparticles/mcp-server calls JSON.parse outside a request-local error boundary in the POST /mcp handler in integrations/mcp-server/src/index.ts. A single unauthenticated malformed JSON body raises a SyntaxError that terminates the Node.js process, leaving the MCP service unavailable until an external supervisor restarts it. This issue is fixed in version 4.3.1.	N/A	More Details
CVE-2026-77372	VeraCrypt provides disk encryption with strong security based on TrueCrypt. Prior to 1.26.30, the Unix, macOS, and FreeBSD serialization paths in src/Platform/Serializer.cpp and src/Volume/VolumePassword.cpp accept untrusted length and count values when deserializing data that can cross from the unprivileged GUI or CLI to the root CoreService helper. Serializer::DeserializeWString allocates floor(size / sizeof(wchar_t)) elements but reads size bytes, so a non-aligned size can overflow the heap allocation. VolumePassword::Deserialize accepts PasswordSize values larger than the fixed 128-byte PasswordBuffer, allowing downstream DataPtr() and Size() consumers such as the KDF to read beyond the buffer. DeserializeString, DeserializeWString, and the string and wide-string list readers also lack allocation and collection bounds, which can exhaust memory, and a zero-length DeserializeString can access an empty vector. Windows uses a different path, and the immediate CoreService pipe writer is the same-user parent process, so the documented exposure is a local defense-in-depth boundary rather than a remote attack. This issue is fixed in 1.26.30.	N/A	More Details
CVE-2026-86041	ezBookkeeping is an open source, self-hosted personal finance application. From 0.10.0 until 1.6.0, ezBookkeeping constructs its Gin router with gin.New() without configuring SetTrustedProxies, causing c.ClientIP() to trust a spoofed X-Forwarded-For value. An unauthenticated remote attacker can supply an allowlisted address to bypass the mcp_allowed_remote_ips or api_token_allowed_remote_ips gate. A valid MCP or API token remains required for protected actions. When such actions occur, the same spoofed value is stored in Transaction.CreatedIp and the request log, attributing activity to the trusted host instead of the attacker. This issue is fixed in version 1.6.0.	N/A	More Details
CVE-2026-109849	Incorrect privilege assignment issue exists in Hinemos. If this vulnerability is exploited, an attacker who can access the password change API with specific permissions that can be assigned to non-administrative users may change the password of an administrative user.	N/A	More Details
CVE-2025-66365	Incorrect handling of SIP packets leads to baseband crashes	N/A	More Details
CVE-2026-122992	In G4KLX DStarGateway and F4FXL DStarGateway before 7b75de6, dstarCallsignToAPRS in APRSUtils.cpp has an integer underflow via an empty RS-MS1A sender field.	N/A	More Details
CVE-2026-123012	In Gogs 0.14.3, the Git Smart HTTP authorization layer in internal/route/repo/http.go allows a push when only read access was intended, a different vulnerability than CVE-2026-52810. This occurs because of a case-sensitivity desync between the authorization classifier and the request dispatcher: the gitHTTPIsPull function compares the Git action verb case-sensitively and defaults to pull (read access) for any unrecognized string, whereas the request dispatcher lowercases the same verb before routing it to the receive-pack handler. Capitalizing a single letter in the URL (e.g. info/Refs instead of info/refs, or git-receive-Pack instead of git-receive-pack) causes the classifier to misidentify a push as a pull, granting only read-level authorization, whereas the dispatcher routes it to the write handler. An authenticated read-only collaborator can exploit this to push to a private repository, creating, updating, or deleting refs.	N/A	More Details
CVE-2026-123014	iTerm2 before 3.7.7beta2 has an argument injection vulnerability in the x-man-page: URL handler, allowing an attacker to execute arbitrary commands with the privileges of the logged-in user by inducing the user to open a crafted URL in iTerm2. Percent-encoded NUL characters survive input sanitization and are subsequently converted to whitespace during command-line parsing, allowing injection of additional arguments to /usr/bin/man. An attacker can inject the -P option to select an attacker-controlled pager command. NOTE: this issue exists because of an incomplete fix for CVE-2023-46321.	N/A	More Details
CVE-2026-123025	An OS Command Injection vulnerability was discovered in the Google Cloud DNS validation module of the OPNsense os-acme-client plugin through 4.17. The DnsGcloud::prepare() method decodes the dns_gcloud_key model field and directly interpolates the string fields gcloud_account and gcloud_project into a shell command passed to proc_open() via LeUtils::run_shell_command() without any validation or escaping. A remote authenticated user with privileges to issue or renew certificates through the WebGUI/API can achieve arbitrary code execution as root.	N/A	More Details
CVE-2026-100109	The Security For WooCommerce WordPress plugin from 1.0.10 to 1.0.16 does not perform capability checks when creating users through an action available to unauthenticated visitors, and lets the caller choose the new account's role, allowing unauthenticated attackers to create administrator accounts and take over the site.	N/A	More Details
CVE-2026-117679	A cross-site scripting vulnerability exists in SHIRASAGI, which may allow an authenticated attacker to execute arbitrary script in a user's web browser when the user accesses a website using the affected product.	N/A	More Details
CVE-2026-113374	Sonatype Nexus Repository 3 does not require realm administration permission when a user creates a Rut Auth capability. A user who holds only the capability creation permission (nexus:capabilities:create) can create this capability, which turns on header-based authentication for the instance. A remote client can then authenticate as an existing user, including an administrator, without credentials.	N/A	More Details

CVE-2026-113372	Sonatype Nexus Repository 3 returns the private signing key of a YUM proxy or group repository to an account that holds only the read privilege for administering that repository. The account does not need the privilege to edit the repository. A party that holds the key can sign repository metadata as that repository.	N/A	More Details
CVE-2026-107479	An integer truncation vulnerability in the QTextCodec conversion functions of the Qt 5 Core Compatibility APIs module impacts the Qt Framework. An application using the affected functionality could crash.	N/A	More Details
CVE-2026-113371	Sonatype Nexus Repository 3 returns the signing passphrase of an APT or YUM repository, through an internal REST endpoint, to a user account that holds only the read privilege for administering that repository. The account does not need the privilege to edit the repository.	N/A	More Details
CVE-2026-118513	Authentication bypass by spoofing in X509Authenticator and X509AuthenticationListener of Symfony versions prior to 5.4.56, 6.x prior to 6.4.50, 7.x prior to 7.4.23, and 8.x prior to 8.1.11 allows an attacker holding a certificate from the application's trusted CA who can influence the CN to authenticate as an arbitrary user of the application, including a privileged one, following an incomplete fix for CVE-2026-45063. X509Authenticator extracts the user identifier from the Subject DN (Distinguished Name) that the web server passes in $_SERVER['SSL_CLIENT_S_DN']. The fix for CVE-2026-45063 anchored that extraction to an RDN (Relative Distinguished Name) boundary, but the regular expression used was not escape-aware. The expression runs against an already serialized DN, so it cannot tell an RDN separator from a separator character that occurs inside a value. Under RFC 2253, used by Apache and by nginx's $ssl_client_s_dn, a comma inside a value is escaped as \, and the expression reads it as a separator regardless. RFC 2253 also does not treat / as a separator, so it leaves it bare inside a value, while the expression treats every / as one. The legacy X509_NAME_oneline() format, used by Apache's LegacyDNStringFormat and by nginx's $ssl_client_s_dn_legacy, is the mirror image: it escapes / as \/ and leaves , bare. In that format, a certificate with no emailAddress attribute, or whose poisoned CN precedes it, authenticates as the smuggled address. To cover both RFC 2253 and the legacy X509_NAME_oneline() format, X509Authenticator and X509AuthenticationListener now split the DN into RDNs before looking for the attribute, instead of matching the attribute against the serialized string. They select the separator from the serialization, split on unescaped occurrences of that separator only, unescape each RDN afterwards with the rules of its format, and require the attribute to span a whole RDN. The accepted value grammar is unchanged. Applications that pass a per-attribute user key (such as SSL_CLIENT_S_DN_Email) and deployments whose CA generates or validates the subject are not affected by this vulnerability.	N/A	More Details
CVE-2026-118516	The Symfony Routing components CompiledUrlMatcher and UrlMatcher interpret the host and path information differently, allowing path-based authorization rules to be bypassed in Symfony versions prior to 5.4.56, 6.x prior to 6.4.50, 7.x prior to 7.4.23, and 8.x prior to 8.1.11. For routes that define a host, CompiledUrlMatcher matches the string $host.'.'.$pathinfo against the host regular expression followed by the path regular expression, while UrlMatcher matches the host and the path separately. A host placeholder can therefore match /, and consume the beginning of the path, so the request is routed to a controller, while UrlMatcher would find no route. Rules that look at the path, such as access_control entries and firewall patterns, are evaluated against the actual request path, so they do not apply while the controller of the route runs, potentially allowing an unauthenticated request to reach a protected controller. For example, with the route /admin/report/{id}, the host app.{domain} and the rule access_control: [{ path: ^/admin, roles: ROLE_ADMIN }], an anonymous request for /admin/report/1 is sent to the login page. A request with the Host header app and path /x./admin/report/1 instead reaches the controller, with domain="/x". With the required domain: .+, the real hostname works: app.example.com and /x./admin/report/1 match with domain="example.com./x". Applications are affected if they have routes with host placeholders protected by path-based rules. With the default requirement, the Host header must be the host of the route without its last labels, such as app: framework.trusted_hosts blocks that, while a web server that only serves known names may not, for instance, Nginx passing the raw Host header to FastCGI for a request line that carries an absolute URI. If the requirement accepts /, such as .+, a real hostname works, and trusted_hosts does not help.	N/A	More Details
CVE-2026-121144	This vulnerability exists in the iRA 2.0 and iRA.ev mobile applications due to presence of hardcoded service account credentials, API Keys and authorization tokens within the application package. An unauthenticated remote attacker could exploit this vulnerability by downloading application package and extracting embedded sensitive information. Successful exploitation of this vulnerability could allow the attacker to gain unauthorized access to associated backend services and potentially access sensitive information or perform unauthorized operations on the targeted system.	N/A	More Details
CVE-2026-121145	This vulnerability exists in the iRA 2.0 and iRA.ev mobile applications due to insufficient validation of URLs and origins loaded within the WebView component. A remote attacker could exploit this vulnerability by sending malicious web content to the affected WebView. Successful exploitation of this vulnerability could allow the attacker to perform unauthorized interaction with application functionality, obtain live bearer authentication tokens and potentially impersonate the associated user and access vehicle related information and services.	N/A	More Details
CVE-2026-121146	This vulnerability exists in the iRA 2.0 and iRA.ev mobile applications due to the recording of authentication tokens in application logs used for development and debugging. A local attacker with an access to logs could exploit this vulnerability by retrieving and misusing the exposed session tokens. Successful exploitation of this vulnerability could allow the attacker to impersonate the associated user and gain unauthorized access to vehicle related information and services.	N/A	More Details
CVE-2026-	This vulnerability exists in the iRA 2.0 and iRA.ev mobile applications due to improper implementation of SSL certificate pinning in the network security configuration, resulting in ineffective certificate pinning controls. An	N/A	More

121147	attacker positioned to intercept network traffic could exploit this vulnerability to intercept or modify communications between the application and its backend services.		Details
CVE-2026-121373	The Symfony HtmlSanitizer component MetaRefreshAttributeSanitizer, introduced to fix CVE-2026-48761, sanitizes the refresh URL of content attributes of meta tags using a regular expression that is too narrow, allowing sanitization to be bypassed, and resulting in potential URL redirection to untrusted sites in Symfony versions 6.1.x prior to 6.4.50, 7.x prior to 7.4.23, and 8.x prior to 8.1.11. The shared declarative refresh steps in the WHATWG HTML Standard require a broader approach: the separator after the time may be ASCII whitespace alone, with no ; or ,, and the url= keyword is optional. Directives the browser honours, but the regular expression misses are returned unchanged, so the attacker URL skips UrlSanitizer entirely and both allowLinkSchemes and allowLinkHosts are defeated for the refresh navigation. This is reachable under any configuration that allows meta with http-equiv and content, including the documented allowStaticElements() preset.	N/A	More Details
CVE-2026-118391	Allocation of Resources Without Limits or Throttling vulnerability in elixir-ecto ecto allows an unauthenticated remote attacker to exhaust memory in the application and in the database server by sending requests with distinct JSON keys or list lengths where the application interpolates them into json_extract_path/2, field[^key] or splice/1. Ecto caches prepared queries per repository in an ETS table with no size limit and no eviction. Interpolated JSON path elements become part of the query expression instead of its parameters, and splice/1 expands into one placeholder per element, so every distinct key or list length creates a new cache entry. With ecto_sql each entry is also a new prepared statement on the database connection that runs it. None of this memory is released until the processes restart. This issue affects ecto: from 3.4.0 before 3.14.3.	N/A	More Details
CVE-2026-119776	In all prior released versions of FRRouting, the OSPFv3 (for IPv6) implementation does not check that OSPFv3 packets have a link-local source address and either a link-local destination or one of the protocol multicast destination groups. This may enable malicious actors to establish OSPFv3 adjacencies from unexpectedly, distant IPv6 hosts. Proper usage of OSPFv3 authentication trailers (RFC 7166, as is best practice) prevents full exploitation of this issue, though may allow a malicious actor to waste CPU on authentication checks. Note the linked PR #23935 is not sufficient to fix the issue as it only verifies the source address. It is the destination address that must be checked. Required configuration: The OSPFv3 for IPv6 routing protocol must be running (ospf6d process) and in use (enabled globally with "router ospf6" and on specific interfaces with "ipv6 ospf6 area".) Workaround: either: * configure OSPFv3 authentication trailers ("ipv6 ospf6 authentication") * or ensure through firewall configuration that only packets with link-local or multicast destination addresses are accepted on input for IPv6 protocol 89 (OSPF). Note that checking the source address is insufficient, as some routers may (unexpectedly) forward packets with global-scoped IPv6 destination addresses even if they have link-local source addresses.	N/A	More Details
CVE-2026-121637	An improper integrity validation vulnerability in WatchGuard AuthPoint Gateway's LDAP authentication callback allows a network attacker who has obtained a valid header signature to forge the authentication result and transaction identifier in the request body, resulting in unauthorized session outcomes.	N/A	More Details
CVE-2026-121638	An Improper Certificate Validation vulnerability in WatchGuard AuthPoint Gateway allows an attacker with an on-path network position to intercept and modify communications between the AuthPoint Gateway and local authentication providers.	N/A	More Details
CVE-2026-121639	A Missing Authentication for Critical Function vulnerability in WatchGuard AuthPoint Gateway allows a remote unauthenticated attacker with network access to the AuthPoint Gateway host to disrupt authentication services and delete the local directory synchronization configuration.	N/A	More Details
CVE-2026-121640	An Authentication Bypass by Capture-replay vulnerability in WatchGuard AuthPoint Gateway allows an attacker who has observed a legitimate request between AuthPoint Gateway components to replay it and perform unauthorized administrative actions, including disrupting authentication services.	N/A	More Details
CVE-2026-66736	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-109518	On Debian, Ubuntu, and derivative Linux distributions, an on-path attacker who can manipulate the HTTP traffic (including a malicious mirror or proxy) between an APT client and an archive server triggered by a package install can trick the client into installing an attacker-controlled unverified package and achieve remote code execution with root privileges. The vulnerability is caused by the reuse of hard links and requires the client to follow redirects and retry the download of package files. It requires the client to have a non-zero Acquire::Retries configuration setting; the value 3 is the default starting with Debian 12 (bookworm) and Ubuntu 22.04 LTS (Jammy Jellyfish), so older releases are unaffected in a default configuration	N/A	More Details
CVE-2026-121971	The component ScopingHttpClient in Symfony HttpClient merges the options of its default scope (such as auth_bearer or auth_basic) into a request before resolving a relative URL against the base_uri, allowing a network-path reference such as "//evil.example/steal" to be sent to another origin together with the default scope’s credentials, and resulting in potential disclosure of those credentials to an attacker-controlled server. This affects Symfony in versions 5.x prior to 5.4.56, 6.x prior to 6.4.50, 7.x prior to 7.4.23, and 8.x prior to 8.1.11. The resolved URL falls outside the origin of the base URI, yet it keeps the merged options, whereas the absolute spelling "https://evil.example/steal" receives none. The same happens with a different port or user-info part on the same host. This is reachable whenever an attacker controls the beginning of a URL passed to a client built with a base_uri and credentials, including those created with HttpClient::createForBaseUri() or configured under	N/A	More Details

	framework.http_client.scoped_clients. To solve the issue, after resolving a relative URL against the base URI of the default scope, ScopingHttpClient now compares the scheme and authority of the result with those of the base URI, parsed the way the request is sent.		
CVE-2026-102345	Zammad is a web based open source helpdesk/customer support system. Prior to 7.1.2, the new Vue-based ticket interface can render ticket article content without the expected output encoding. An authenticated user can store markup in an article that is interpreted when another user views the ticket, enabling stored cross-site scripting. The default Content Security Policy limits practical impact, and the classic REST/CoffeeScript interface is not affected. This issue is fixed in version 7.1.2.	N/A	More Details
CVE-2026-107846	bitcoinjs-lib is a JavaScript Bitcoin library for Node.js and browsers. From 2.3.0 until 5.2.1, 6.1.8, and 7.0.2, fastMerkleRoot pads odd Merkle-tree levels by hashing the final node with itself but does not report adjacent duplicate hashes. The affected block-root verifier was introduced as Block.checkMerkleRoot() alongside Block.calculateMerkleRoot(), while later versions expose validation through checkTxRoots() and __checkMerkleRoot; these validation paths can accept a recomputed root without checking for mutation. A peer can append duplicate transactions so a different transaction list retains the original Merkle root, block header, proof of work, and block identifier. Consumers that rely on block-root validation, including explorers, exchange indexers, or SPV clients, can process a duplicated transaction twice or blacklist the shared block hash and reject the honest block. This issue is fixed in versions 5.2.1, 6.1.8, and 7.0.2.	N/A	More Details
CVE-2026-122148	In Yealink MeetingBoard Pro before 331.320.0.64, the Web management module has a front-end validation bypass vulnerability. An attacker with administrator privileges can modify the page DOM to bypass front-end UI control logic and invoke screenshot-related interfaces, triggering the screenshot function by circumventing front-end interface restrictions. Exploitation can occur only when the attacker has a valid administrator account within the local network.	N/A	More Details
CVE-2026-63183	OmniAuth is a flexible authentication system utilizing Rack middleware. Prior to 2.2.0, OmniAuth derives provider callback URLs from request-controlled host information when neither a fixed full_host nor framework-level incoming host validation is configured. A remote unauthenticated client can supply a forged Host header, creating a host header injection risk in applications whose web framework does not verify incoming host headers. Applications using appropriately configured Rails host authorization or a fixed full_host are not affected by this path. This issue is fixed in version 2.2.0.	N/A	More Details
CVE-2026-113368	Sonatype Nexus Repository 3 does not check that a user account is authorized to access a repository before the repository is added as a member of a group repository. A user account that has signed in with valid credentials and holds the add or edit privilege on a group repository can add a repository that the account cannot read or browse, and then read the content of that repository through the group. The anonymous user can only do this if an administrator has explicitly granted it that privilege.	N/A	More Details
CVE-2026-113369	Sonatype Nexus Repository 3 allows a user account that can push manifests to a hosted OCI repository (a user account that holds the edit permission on that repository) to store script content in the artifact type field of an OCI manifest. The script runs in the browser of a user who opens the Attestations tab for the related image in the Browse user interface, with the permissions of the viewing user.	N/A	More Details
CVE-2026-113370	Sonatype Nexus Repository 3 contains a SQL injection vulnerability in the optional "Reindex Search Tables By Pattern" task. A user who holds the nexus:tasks:create privilege can supply a crafted filter condition that the database runs as SQL. This allows the user to modify data in the Nexus database. The task is available only when the non-default setting nexus.reindex.search.by.pattern.visible is set to true.	N/A	More Details
CVE-2020-29114	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29115	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29116	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2026-111062	russh is a Rust SSH client and server library. From version 0.34.0-beta.1 until version 0.64.0, its SSH server does not require the signature algorithm in a public-key authentication signature to match the algorithm named in the authentication request. A client possessing an authorized RSA private key can announce rsa-sha2-512 while supplying a valid ssh-rsa SHA-1 signature, bypassing restrictions or producing misleading audit records when applications rely on the requested algorithm. A valid private-key signature remains required, and russh clients are not affected. This issue is fixed in version 0.64.0.	N/A	More Details
CVE-2026-114134	Black is the uncompromising Python code formatter. Prior to 26.10.1, the Black GitHub Action with use_pyproject: true accepts tool.black.required-version from pyproject.toml without validating that it is a released Black version specifier. An attacker who can submit a pull request can change that field to a direct reference to attacker-controlled code, causing the workflow to install and execute the code in the victim repository's GitHub Actions context. This issue is fixed in version 26.10.1.	N/A	More Details

CVE-2026-114604	GraphQL Tools provides utilities for building, stitching, and mocking GraphQL schemas. From 10.10.1 until 12.0.2, the @graphql-tools/utils mergeIncrementalResult helper passes incrementalResult.path segments to setObjectKeyPath without runtime primitive-type validation. A non-primitive segment can bypass strict comparisons against __proto__, constructor, and prototype, then be coerced during property access so a malicious or compromised upstream incremental GraphQL response writes attacker-controlled properties to Object.prototype in the consuming Node.js process. The affected implementation is packages/utils/src/mergeIncrementalResult.ts and is reachable when consumers merge untrusted @defer or @stream transport results. This issue is fixed in version 12.0.2.	N/A	More Details
CVE-2026-34157	Wails is a framework for building desktop applications using Go and web technologies. From 2.0.0 until 2.13.0, BindingsAllowedOrigins in v2/internal/frontend/originvalidator/originValidator.go passes wildcard patterns to wildcardPatternToRegex, which expands every asterisk to an unrestricted regular-expression match. When an application configures a trailing or partial-label wildcard immediately after an allowed domain, an attacker-controlled lookalike origin can match the allowed suffix and invoke bound Go methods through IPC. A complete-component subdomain wildcard is an unaffected configuration. The resulting confidentiality, integrity, and availability impact depends on the file, database, command, credential, or other operations exposed by the application's bound methods. This issue is fixed in version 2.13.0.	N/A	More Details
CVE-2026-55458	Caddy is an extensible server platform that uses TLS by default. Prior to 2.11.5, the reverse proxy's finalizeResponse method in modules/caddyhttp/reverseproxy/reverseproxy.go handles an upstream 101 Switching Protocols response before running removeConnectionHeaders and the hopHeaders deletion loop used for ordinary responses. The early return invokes handleUpgradeResponse, which copies the upstream headers to the client and normalizes only WebSocket-specific header names. An attacker who controls or compromises a proxied WebSocket upstream can therefore cause hop-by-hop headers such as Alt-Svc, Keep-Alive, and Proxy-Authenticate, as well as headers named by Connection, to cross the proxy boundary. For HTTP/2 or HTTP/3 extended CONNECT, the upstream 101 response may be represented to the client as an ordinary successful response, increasing the chance that leaked headers are processed. This issue is fixed in version 2.11.5.	N/A	More Details
CVE-2026-62268	borgbackup is an opensource, deduplicating archiver with compression and authenticated encryption. Prior to 1.4.5 and 2.0.0b22, extracting a malicious archive can follow a symlinked parent path or resolve embedded dot-dot path components and delete or overwrite files outside the extraction directory. A crafted slave hardlink can also use an attacker-controlled hardlink source outside the extraction directory and hard-link that file into the restored tree, disclosing its contents. Creating the malicious archive requires repository access and, for encrypted or authenticated repositories, the Borg key and passphrase; a victim must then extract the archive. This issue is fixed in versions 1.4.5 and 2.0.0b22.	N/A	More Details
CVE-2026-69143	Rejected reason: This CVE is a duplicate of another CVE.	N/A	More Details
CVE-2026-77622	Sliver is a command and control framework. Prior to 1.7.6, an HTTP(S) listener using the PNG encoder accepts attacker-controlled PNG dimensions without an effective decoded-size or pixel limit in util/encoders/images.go, while the listener nonce space implemented in server/encoders/encoders.go is small enough to search remotely. An unauthenticated attacker who identifies a valid nonce can submit a highly compressed image to PNGEncoder.Decode, where it expands during png.Decode, exhausting server memory and causing a complete loss of availability. This vulnerability is fixed in 1.7.6.	N/A	More Details
CVE-2026-81190	KurrentDB is a database engineered for modern software applications and event-driven architectures. In version 26.1.0, a user authorized to read the $all stream can use Secondary Indexing query capabilities to read arbitrary files accessible to the database process, enumerate directories, and issue HTTP GET requests from that process. The default configuration limits this privilege to administrators. The flaw does not permit file writes and does not expose environment variables. This issue is fixed in version 26.1.1.	N/A	More Details
CVE-2026-85076	Cronicle is a multi-server task scheduler and runner, with a web based front-end UI. Prior to 0.9.124, an authenticated non-admin with run_events, create_events, or edit_events privilege can supply undeclared keys in event params through api_create_event, api_update_event, or api_run_event. lib/api.js and lib/api/event.js validate the parameter object without restricting its keys, and lib/job.js uppercases those keys and applies them to the child process environment after administrator-defined plugin variables. A key that collides with a security-sensitive environment variable can therefore override the plugin execution context and may cause privilege escalation, arbitrary code execution, data access, or service disruption depending on the plugin and runtime. This issue is fixed in version 0.9.124.	N/A	More Details
CVE-2026-100395	LXC is a userspace interface for the Linux kernel containment features used to create and manage system containers. In LXC 7.0.0 and earlier, lxc-copy and the public liblxc clone() API can follow attacker-controlled symbolic links while updating /etc/hostname in a copied container root filesystem. The affected surfaces are lxc-copy and liblxc's public lxc_container::clone() API. The privileged cloning process must run as root. The source rootfs must be attacker-controlled or less trusted. A symlink can be placed at etc/hostname or in an intermediate component. The clone operation preserves the symlink before updating the hostname. The vulnerable write truncates and overwrites an existing file outside the destination rootfs. When root clones an untrusted container without LXC_CLONE_KEEPNAME, the copied symlink can resolve outside the destination rootfs and cause the privileged process to overwrite an existing host file with the destination container name. Unprivileged use and managers with independent cloning implementations are not affected. LXC_CLONE_KEEPNAME avoids the hostname update and therefore the affected write.	N/A	More Details

CVE-2026-111489	A static credential embedded in the mobile app has been reported to return the 'autorizado' token on the MatchPoint platform. The report states that this token grants unauthenticated access to API services.	N/A	More Details
CVE-2026-111490	Insecure direct object reference (IDOR) vulnerability in the MatchPoint API, which relies on the `actingasuser` HTTP header without verifying the requester's authorization for the specified user. Manipulation of sequential identifiers allows access to personal, banking, and financial data, private messages, and QR codes for physical access, as well as the ability to modify third-party accounts, change passwords, impersonate users, and transfer virtual balances.	N/A	More Details
CVE-2026-111491	Credentials are stored in plain text in an SQLite database and in the MatchPoint Android app's SharedPreferences. An attacker with access to the device's local data or a backup could retrieve usernames and passwords and use them to gain unauthorized access to accounts on the platform.	N/A	More Details
CVE-2026-111492	SQL injection in the push notification handler of the MatchPoint Android app, which processes messages from Firebase Cloud Messaging and constructs queries by concatenating untrusted data. An attacker capable of interacting with the component could manipulate queries and access sensitive information from the local database, including credentials stored in the versions described in the report. The scope of the injection is limited to the device.	N/A	More Details
CVE-2026-111493	Lack of authentication and authorization in the Images.ashx endpoint in MatchPoint, which allows profile photos to be downloaded using predictable identifiers. An unauthenticated remote attacker could enumerate these identifiers and collect users' photos. Linking these photos to identities may be facilitated by other vulnerabilities in the platform.	N/A	More Details
CVE-2026-111494	Incorrect validation of TLS certificates in the MatchPoint Android app due to a TrustManager that accepts any certificate and a permissive hostname validator. Additionally, the app allows unencrypted HTTP traffic. An attacker capable of intercepting the victim's traffic could read and modify communications, including credentials and personal data.	N/A	More Details
CVE-2026-111495	API keys, credentials, and configuration parameters embedded in the MatchPoint APK, which can be extracted through reverse engineering. The vendor distinguishes the extracted elements from Google Maps and Firebase keys that must remain on the client side and considers them project identifiers, not authentication secrets. The impact depends on the capabilities and restrictions of each exposed element.	N/A	More Details
CVE-2026-122267	MinIO Signature V4 verification before RELEASE.2026-09-22T19-25-18Z accepts unsigned x-amz-* headers, letting a presigned PUT URL be escalated into a cross-bucket read.	N/A	More Details
CVE-2026-110390	Missing authentication in the FlexNet Beacon component of Flexera One and FlexNet Manager Suite allows unauthenticated remote attackers to obtain Beacon policy and targeting information when anonymous web server access is enabled (the default).	N/A	More Details
CVE-2026-16579	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-88984	Kubeflow Pipelines enables users to build and deploy portable, scalable machine learning workflows. Prior to 2.16.1, the multi-user API server treats the empty namespace used by shared or global pipelines as an authorization exception for modification and deletion operations. An authenticated user can modify or delete shared pipeline definitions and versions without the required Kubernetes RBAC permissions, compromising their integrity and availability. Read-only access to shared pipelines remains intentional, single-user deployments intentionally bypass multi-user checks, and execution of a modified pipeline is a conditional downstream consequence. The separate shared-pipeline multipart upload authorization path is outside this advisory and is not remediated by version 2.16.1. This issue is fixed in version 2.16.1.	N/A	More Details
CVE-2026-107492	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-114366	An information disclosure vulnerability in the Qt Framework QWebSocket authentication handling of the Qt WebSockets module.	N/A	More Details
CVE-2026-111753	Angular is a development platform for building mobile and desktop web applications using TypeScript/JavaScript and other languages. Prior to 20.3.34 and 21.0.3, the @angular/common HttpClient function xsrfInterceptorFn uses a regular expression that does not normalize request URLs in the same way as the browser's WHATWG URL parser. With XSRF protection enabled, a mutating HTTP request to an attacker-controlled URL containing backslashes, stripped control characters or spaces, or removable ASCII whitespace can be misclassified as relative and same-origin, causing the interceptor to attach the X-XSRF-TOKEN header before the browser dispatches the request to a cross-origin host. With permissive CORS handling for the custom header, the attacker can obtain the victim's XSRF token and use it to perform cross-site request forgery against the victim session. This issue is fixed in versions 20.3.34 and 21.0.3.	N/A	More Details
	libwebsockets MQTT Protocol PUBACK Packet Handling Out-Of-Bounds Write Remote Code Execution Vulnerability.		

CVE-2026-114550	This vulnerability allows remote attackers to execute arbitrary code on affected installations of libwebsockets. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of PUBACK packets. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-31039.	N/A	More Details
CVE-2026-121819	A vulnerability has been identified in armeria-xds versions 1.40.0 through 1.42.0, where DataSourcePolicy checks filename containment without resolving symbolic links, allowing a compromised or semi-trusted xDS control plane to cause the xDS client to read files outside configured allowed root directories when a symbolic link inside an allowed directory points outside it. In deployments using a credential injector, header-compatible text secrets may be exposed to an attacker-observable upstream.	N/A	More Details
CVE-2026-118494	Joomla Extension - jreviews.com - Secret configs cached in a web-accessible in JReviews 1.0.0-5.12.0, 6.0.0-6.6.9 - JReviews caches its full settings table, including the Joomla global configuration secret (copied into cms_secret) and third-party API keys and secrets, to a serialized file under components/com_s2framework/tmp/cache/core/ inside the web root. The file has no PHP guard and the directory has no .htaccess, so anyone who knows the file name can read it without authentication.	N/A	More Details
CVE-2023-44364	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2023-44368	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2023-44369	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2023-44370	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2023-47045	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2023-47082	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2023-47083	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2023-47084	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2023-47085	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2023-47086	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2023-47087	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2023-47088	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2023-47089	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2023-51465	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-			More

2023-51466	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	Details
CVE-2026-119344	Cocos AI is a confidential computing system for AI. In version 0.8.2 and earlier, Cocos AI accepts trusted execution environment attestation Evidence when firmware patch levels and software measurements match, without binding the Evidence to an allowed platform owner or unique machine identity and without enforcing revocation. A remote attacker who controls or compromises another platform trusted by the same verifier can substitute valid Evidence from that platform and cause authorization of the wrong platform. This vulnerability is addressed in 0.9.0. However, this vulnerability can't be patched in source code alone, since the vulnerability arises from the confidential computing threat model itself.	N/A	More Details
CVE-2026-119345	Cocos AI is a confidential computing system for AI. Prior to 0.9.0, Cocos AI performs attestation only once when an attested TLS connection is established. An attacker who can modify the attester's workload code, memory-backed state, configuration, or attached devices after that check can keep the existing connection open while the peer continues trusting stale initial Evidence. This gap is especially significant for long-lived connections because the verifier has no mechanism to detect the changed state. This issue is fixed in version 0.9.0.	N/A	More Details
CVE-2026-70660	stable-diffusion.cpp is a pure C/C++ library for running diffusion model (Stable Diffusion, Flux, Wan, Qwen Image, Z-Image, and more) inference. Prior to master-764-e22272e, the safetensors loader in src/model_io/safetensors_io.cpp trusts each tensor's data_offsets after checking only that nbytes equals end - begin. A crafted .safetensors file can declare a byte range beyond the file's data section, causing src/model_loader.cpp to consume an attacker-chosen length from an unchecked mapped-file offset. Loading the model can read adjacent process memory into tensor buffers or crash the process. This issue is fixed in master-764-e22272e.	N/A	More Details
CVE-2026-102927	HedgeDoc is an open source, real-time collaborative markdown notes application. Prior to 1.11.1, the WebSocket permission handler allows a note owner to store strings outside the supported freely, editable, limited, locked, protected, and private permission values. The viewing and editing checks handle only known values and can otherwise fall through to permissive behavior, making a note readable or writable more broadly than intended. SQLite deployments can persist the invalid value because the database column does not strictly enforce the set, while MySQL and PostgreSQL reject the database update but can leave the in-memory note state inconsistent for connected users until reload or cache eviction. Exploitation requires the note owner to intentionally submit an invalid permission value, and the owner could already choose a legitimate permissive setting, which limits the practical security impact. This issue is fixed in version 1.11.1.	N/A	More Details
CVE-2026-107130	Joomla Extension - balbooa.com - Unauthenticated deletion of submission/field files in Gridbox < 2.20.5.0	N/A	More Details
CVE-2026-54912	WebAssembly Micro Runtime (WAMR) is a lightweight standalone WebAssembly (Wasm) runtime. Prior to 2.4.5, the two-pass fast interpreter loader in core/iwasm/interpreter/wasm_loader.c can make inconsistent constant-table decisions between the sizing pass and the emitting pass. After duplicate constants inflate the first pass beyond the constant-slot limit, wasm_loader_get_const_offset emits later constants inline, but the between-pass sort and deduplication reduces the table so the second pass can choose table references and cause reserve_block_ret to emit additional copy operands that were not included in code_compiled_peak_size. A crafted module can therefore make the second pass write partially attacker-controlled compiled-code data beyond the heap buffer allocated from the first pass's size calculation during wasm_runtime_load, before guest code executes. This can corrupt host heap metadata and deterministically crash the process, causing denial of service; further consequences depend on the host application's heap layout. Builds using WAMR_BUILD_FAST_INTERP=1 are affected; disabling the fast interpreter avoids the vulnerable loader. This issue is fixed in version 2.4.5.	N/A	More Details
CVE-2026-54913	WebAssembly Micro Runtime (WAMR) is a lightweight standalone WebAssembly (Wasm) runtime. Prior to 2.4.5, load_init_expr in core/iwasm/interpreter/wasm_loader.c accepts a non-reference heap-type byte for ref.null when WASM_ENABLE_GC=0, while the local WASMValue cur_value union is not zero-initialized and setting ref_index writes only part of it. A crafted module can declare an i64, f64, or v128 global initialized through the invalid ref.null form, causing push_const_expr_stack and the later global initialization path to copy uninitialized host-stack bytes into a value readable by the guest. The classic and fast interpreters are affected in the default no-GC configuration; the GC-enabled path validates heap types. The disclosure is four bytes for i64 or f64 globals and up to twelve bytes for each v128 global. This issue is fixed in version 2.4.5.	N/A	More Details
CVE-2026-54914	WebAssembly Micro Runtime (WAMR) is a lightweight standalone WebAssembly (Wasm) runtime. Prior to 2.4.5, wasi_poll_oneoff in core/iwasm/libraries/libc-wasi/libc_wasi_wrapper.c validates the output pointer for only one wasi_event_t, while wasmtime_ssp_poll_oneoff in core/iwasm/libraries/libc-wasi/sandboxed-system-primitives/src/posix.c can write as many events as the guest-controlled nsubscriptions value. A crafted guest module can provide multiple subscriptions that produce events while positioning an output region large enough for only one event, causing a later out[nevents] write to cross the validated Wasm linear-memory boundary into adjacent host heap memory. The overwrite contains partly attacker-controlled event data and can reliably crash the host process, with further confidentiality or integrity consequences depending on heap layout. This issue is fixed in version 2.4.5.	N/A	More Details
CVE-2026-83494	A flaw was found in the training-operator. An incorrect object casting in the PyTorchJob ValidateUpdate webhook allows users to bypass an immutability check. This vulnerability could enable users to detach a queued job from its quota management system or hijack a running job's controller ownership. The primary impact is a Denial of Service (DoS) condition.	N/A	More Details

CVE-2026-121820	A vulnerability has been identified in armeria-saml versions prior to 1.43.0, where the HTTP-Redirect binding decoder decompresses attacker-supplied SAML messages without limiting the output size before signature validation, allowing an unauthenticated remote attacker to exhaust server memory and cause a denial of service.	N/A	More Details
CVE-2020-29117	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2026-111573	Incorrect permissions on the Checkmk Windows agent's data directory, caused by a race condition that discards the permission changes during service start, in Checkmk <2.5.0p18, <2.4.0p39, <2.3.0p52 and 2.2.0 (EOL) allow a local user to execute arbitrary code as SYSTEM by placing scripts in the agent's plugins or local folders, and to read the agent controller's private key.	N/A	More Details
CVE-2026-121880	Authorization bypass through user-controlled key in the localhost port-proxy (/p/<token>/) in Posit Software, PBC RStudio Server and Posit Workbench before 2026.08.0 allows remote authenticated users to reach web applications and other services bound to 127.0.0.1 under a different user's session, and to view their live rendered content and data, via a proxy URL constructed from the attacker's own port token for an arbitrary port number. The port token is a documented obfuscation measure and not an authorization boundary, and the proxy does not verify that the requested port belongs to the requesting user's session. NOTE: exploitation requires an authenticated account on the same multi-user server and a target service listening on localhost at the time of access. Impact may be greater on hosts that co-locate additional privileged localhost services, and the bypass is not prevented by allow-shell=false; no setting restricts the port-proxy without disabling all application proxying.	N/A	More Details
CVE-2026-121881	SQL injection vulnerability in the get_last_seen code-server session-state RPC in Posit Software, PBC Posit Workbench before 2026.08.0 allows authenticated users to read arbitrary data from the Workbench database via the sessionIds parameter. NOTE: exploitation requires a valid authenticated session; no administrative privileges are needed. The vulnerability is limited to disclosure of database contents.	N/A	More Details
CVE-2026-123792	The Symfony Yaml components Inline and Parser, parse some YAML documents inefficiently, so that a small crafted document can take disproportionately long to process, keeping a PHP process busy for seconds or minutes, potentially causing a denial of service in Symfony versions prior to 5.4.56, 6.x prior to 6.4.50, 7.x prior to 7.4.23, and 8.x prior to 8.1.11. The parser repeats work it has already done in several places. An embedded mapping in a flow sequence is parsed again for every scalar appended to it, and so are the collections nested in it, so the parse time grows exponentially with the nesting depth. The patterns matching mapping keys and tags scan a run of spaces once per character of the run, and each scalar of a flow collection is matched against a copy of the rest of the collection, so the parse time grows quadratically with the size of the input. Nested blocks are also copied at each nesting level, which consumes memory as well as time. A few other constructs, such as an empty sequence item followed by a blank line or an anchor named 0, trigger similar repeated work. Any code parsing untrusted YAML is affected, with the default flags. In Symfony 7.4 and later, that includes #[MapRequestPayload] when the Yaml component is installed and the endpoint does not restrict acceptFormat. A single unauthenticated request with a YAML content type keeps a PHP worker busy until max_execution_time. JSON documents are valid YAML, so a JSON payload sent with a YAML content type is enough for the flow collection case. In Symfony 6.4, #[MapRequestPayload] accepts YAML only when the application registers a yaml request format.	N/A	More Details
CVE-2026-118515	The Symfony Serializer component DataUriNormalizer handles only the exact types SplFileInfo, SplFileObject, and File, so for a property typed with a subclass such as UploadedFile, ObjectNormalizer instantiates the object through its constructor from attacker-controlled data, including the file path. This allows an arbitrary file on the server to be treated as an uploaded file in Symfony versions prior to 5.4.56, 6.x prior to 6.4.50, 7.x prior to 7.4.23, and 8.x prior to 8.1.11. A request body such as {"image": {"path": "/path/to/project/.env.local", "originalName": "a.png", "test": true}} makes the application handle any file on the server as an upload, without the file being sent. With test: true, UploadedFile::isValid() skips is_uploaded_file() and move() falls back to rename(). Assert\File does not prevent this because it validates the file at the attacker-chosen path, which exists on the server. Any code that deserializes untrusted data into a type that holds such a property is affected. That includes #[MapRequestPayload] on a DTO with an UploadedFile property, which is how uploads are mapped in Symfony 8.1; a single unauthenticated request with a JSON or form body is enough. Depending on what the application does with the upload, this can expose any file readable by PHP (for instance, when uploads are stored and served back), move any such file when move() is called, and reveal whether a path exists. A serializer built without DataUriNormalizer ahead of the object normalizer is not protected by the fix; the serializer configured by FrameworkBundle is.	N/A	More Details
CVE-2024-36240	Rejected reason: Unused reservation with no CVE record; removed from tickets/pool during the 2026-11-06 stale-CVE remediation	N/A	More Details
CVE-2025-46896	Rejected reason: Unused reservation with no CVE record; removed from tickets/pool during the 2026-11-06 stale-CVE remediation	N/A	More Details
CVE-2025-64798	Rejected reason: Unused reservation with no CVE record; removed from tickets/pool during the 2026-11-06 stale-CVE remediation	N/A	More Details

CVE-2026-100080	In the Linux kernel, the following vulnerability has been resolved: xen-netback: Fix UAF when reading statistics data The network statistic data in the driver is protected by RCU. Unfortunately when tearing down the queues after an error during connecting to the frontend (e.g. due to illegal Xenstore data filled in by the guest), the statistic data is being freed without synchronizing the RCU state. In case the data is being read via sysfs in this phase, access to already freed memory or memory being in new use is possible. Fix that by calling synchronize_net() before freeing the queue data. This is XSA-526 / CVE-2026-100080	N/A	More Details
CVE-2026-100082	In the Linux kernel, the following vulnerability has been resolved: xen-blkback: Avoid UAF when reading I/O statistics Reading I/O statistics via sysfs concurrently with tearing down a frontend device might result in UAF or a NULL dereference, as the reading of the statistics data is not synchronized with freeing the data. Use a rwlock for synchronizing. This is XSA-528 / CVE-2026-100082	N/A	More Details
CVE-2026-10146	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-10147	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-47400	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-47401	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-47402	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-47403	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-47404	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-49122	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-49123	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-49124	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-49125	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-49126	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-56717	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-109683	A newline injection vulnerability exists in the UPnP service of Archer BE805 v1 such that an adjacent attacker can supply newline characters in a UPnP port-mapping description due to improper sanitization, resulting in possible injection of unintended content into UPnP port-mapping data. Successful exploitation may allow an unauthenticated attacker on the local network to modify runtime UPnP port-mapping information and create spoofed entries within the affected service. The issue is limited to the integrity of UPnP mapping data and does not demonstrate code execution or privilege escalation.	N/A	More Details
CVE-	The Symfony Serializer component DataUriNormalizer::denormalize() matches the data: scheme with a case-sensitive regular expression, allowing a value with an uppercase scheme, such as DATA:,/../../../etc/passwd, to bypass it, resulting in Arbitrary Local File Read through Path Traversal in Symfony versions prior to 5.4.56, 6.x prior to 6.4.50, 7.x prior to 7.4.23, and 8.x prior to 8.1.11. A value whose scheme is not lowercase data: are		

2026-121623	treated as a local file path and opened instead of being decoded as inline data, so the resulting File, \SplFileInfo, or \SplFileObject points at a file on the server, which the application then handles as the uploaded content. Any endpoint that deserializes untrusted input into one of these types is affected. FrameworkBundle registers DataUriNormalizer ahead of ObjectNormalizer by default. A single request with a crafted DATA: value is enough to read arbitrary local files that the application can access, with no authentication needed if the endpoint is public.	N/A	More Details
CVE-2026-64894	Inclusion of functionality from untrusted control sphere vulnerability in Johnson Controls EasyIO Neo IOManager and Tools Installer allows Malicious Software Update. This issue affects EasyIO Neo IOManager and Tools Installer: 1.1.0.0.	N/A	More Details
CVE-2026-121821	A vulnerability has been identified in armeria versions 0.84.0 through 1.42.0, where any-origin CORS policies do not enforce configured path restrictions, allowing an attacker-controlled website visited by an authenticated victim to read sensitive responses from excluded paths when credentials are enabled and the victim's browser sends authentication credentials.	N/A	More Details
CVE-2026-123339	Improper trust of forwarded headers in RouterListener::onKernelFinishRequest() in Symfony HttpKernel versions prior to 5.4.56, 6.x prior to 6.4.50, 7.x prior to 7.4.23, and 8.x prior to 8.1.11 allows a remote attacker to control the host, scheme, and port of absolute URLs generated for the rest of the request, poisoning links in pages stored by a shared cache and in e-mails sent after the page was rendered.When a page renders an inline fragment (render() in Twig, or an ESI tag rendered inline), SubRequestHandler temporarily adds 127.0.0.1 to the trusted proxies, and RouterListener rebuilds the router context from the main request while that trust is still active, so the X-Forwarded-* and Forwarded headers of a request whose client address is 127.0.0.1 are trusted even though that address is not a configured trusted proxy. From that point on, every absolute URL the router generates for the rest of the main request takes its host, scheme, and port from headers sent by the client, including URLs produced by url() in Twig and by UrlGeneratorInterface::ABSOLUTE_URL. Applications are affected when they are reached over HTTP from 127.0.0.1, for example behind a TLS terminator, reverse proxy, local HTTP cache, or sidecar proxy on the same host, and that proxy passes the client’s forwarded headers along. With the default configuration (framework.trusted_proxies unset), all forwarded headers, including X-Forwarded-Host, are trusted during that window. Applications served through php-fpm, mod_php, or a proxy on another host are not affected. When framework.trusted_hosts is configured, a forwarded host outside the list is rejected, but the scheme and port can still be changed.	N/A	More Details
CVE-2026-121822	A vulnerability has been identified in armeria versions 0.80.0 through 1.42.0, where attackers who control file names can cause stored cross-site scripting (XSS) when directory listing is enabled and a user views the listing.	N/A	More Details
CVE-2026-121823	A vulnerability has been identified in armeria versions prior to 1.43.0, where inconsistent request path normalization can allow unauthenticated attackers to bypass path-based access controls and access protected resources.	N/A	More Details
CVE-2026-121824	A vulnerability has been identified in armeria versions prior to 1.43.0, where processing malformed Thrift messages can cause excessive memory allocation, potentially resulting in denial of service.	N/A	More Details
CVE-2026-103674	Invocation of the NetApp ONTAP special agent with the login password in the command line in Checkmk version 2.5.0 before 2.5.0p16 allows a local user on the Checkmk server to read the NetApp login password from the process list while the special agent is running. This affects both explicitly configured passwords and passwords from the password store.	N/A	More Details
CVE-2026-103682	Invocation of the Jolokia special agent with the login password in the command line in Checkmk versions 2.5.0 before 2.5.0p16 allows a local user on the Checkmk server to read the Jolokia login password from the process list while the special agent is running. This affects both explicitly configured passwords and passwords from the password store.	N/A	More Details
CVE-2026-123660	In Vulnerability-Lookup 5.5.1 up to but not including 6.4.1, a signed-in user could make the server allocate memory far out of proportion to their input through a webhook notification's payload template. Each placeholder's format specifier was passed unchanged to Python's string formatting, which builds the padded result before its size can be checked. A template of a few dozen bytes, such as {"text": "{title:>999999999}"}, therefore produced a string of about 1 GB when the notification form test-rendered it on save, and repeating such fields multiplied the cost. Templates that passed the save check could also repeat placeholders such as {text} thousands of times; the notification daemon rebuilt those on every webhook delivery. Deeply nested templates raised an unhandled recursion error (HTTP 500). An attacker needs only an account, which the default configuration lets anyone create after e-mail confirmation. They could exhaust the memory of web workers or the notification daemon, causing a denial of service. Version 6.4.1 caps every number in a format specifier at 256, limits a rendered template to 1,000,000 characters both on save and at delivery, and rejects templates nested deeper than 32 levels.	N/A	More Details
CVE-2026-123087	SQL injection vulnerability in Atmira’s SIREC. The server retrieves the value of a field from a JSON object containing user-supplied information and concatenates it into an SQL statement without properly sanitising the input. This allows the original query to be altered via malicious input, causing the database to return unexpected information.	N/A	More Details
	Allocation of Resources Without Limits or Throttling vulnerability in ninenines cowlib allows an unauthenticated remote peer to exhaust the memory of an HTTP/2 endpoint via HPACK-indexed header fields.		

CVE-2026-113431	cow_http2_machine:headers_decode/4 in src/cow_http2_machine.erl decodes every HEADERS block with cow_hpack:decode/3. It bounds the compressed block size and the number of fields, but not the size of the decoded header list that RFC 9113 section 6.5.2 places under SETTINGS_MAX_HEADER_LIST_SIZE. A peer stores one header value of up to the dynamic table size (4096 bytes by default) and then references it with one-byte indexed fields, so about 100 bytes on the wire decode to a header list of about 390 KB. A consumer that copies the decoded values, as Cowboy does when cowboy_http2:headers_to_map/2 joins repeated cookie fields into one binary, allocates that amount for every stream. The total across streams and connections is not bounded. This issue affects cowlib: from 2.7.0 before 2.22.0.	N/A	More Details
CVE-2026-115701	Allocation of Resources Without Limits or Throttling vulnerability in ninenines cowboy allows an unauthenticated remote attacker to exhaust connection process memory over HTTP/1.1. Once a request has been received in full and its handler is still running, cowboy_http:parse/2 in src/cowboy_http.erl appends every further byte that arrives on the keep-alive connection to the connection buffer and returns to the receive loop without parsing it. The socket stays in active mode and no limit applies to this buffer: max_request_line_length, max_headers and the other parser limits only take effect once the handler returns and parsing resumes, and the only timer in this state is idle_timeout (default 60 seconds), which is reset on every received chunk. A client can therefore send an arbitrary amount of data on one connection for as long as the handler runs, and a few connections to an endpoint that holds requests open can drive the Erlang VM into out-of-memory conditions. This issue affects cowboy: from 2.18.0 before 2.21.0.	N/A	More Details
CVE-2026-66293	XML injection in the encoder of Saxy. Saxy.Encoder does not neutralize the -- sequence in XML comment content: escape_comment/2 returns the comment binary unchanged in every clause and only appends a space when the comment ends in a single -, so neither an interior -- nor a full --> is escaped or rejected before the encoder wraps the content in the <!-- and --> delimiters. When an application serializes attacker-controlled text as a comment, through Saxy.XML.comment/1 or a raw {:comment, text} simple form child, the attacker can close the comment early with --> and inject arbitrary sibling markup into the serialized document. A downstream parser then sees elements, attributes, and text that the application never built. Where the document is rendered as HTML or SVG, the injected markup executes as stored cross-site scripting; where it is consumed by another XML processor, the attacker can forge data that the producing application never emitted. Documents that Saxy only parses are not a vector. This issue affects saxy: from 0.7.0 before 1.7.0.	N/A	More Details
CVE-2026-66294	XML injection in the Saxy XML encoder. Saxy.Encoder.cdata/1 serializes a {:cdata, characters} node by wrapping the supplied characters between <![CDATA[and]]> and passing the payload through byte for byte. The encoder's character-data and attribute-value paths escape the XML metacharacters <, >, &, ", and ', but the CDATA path applies no neutralization at all. XML provides no character escaping mechanism inside a CDATA section, so the only correct way to represent a]]> substring is to split the section and rejoin it as]]]]><![CDATA[>. Saxy neither performs that split nor rejects the substring. An application that renders untrusted text as CDATA, by building the node with Saxy.XML.cdata/1 and serializing it with Saxy.encode!/2 or Saxy.encode_to_iodata!/2, therefore lets an attacker terminate the section at a position of their choosing. Everything supplied after the]]> is emitted outside any CDATA context and is parsed as markup, so a single attacker-controlled text field becomes attacker-controlled document structure: arbitrary sibling elements and attributes that the application never built. Downstream consumers of the serialized document accept the injected markup as genuine. Services that generate SOAP envelopes, RSS or Atom feeds, sitemaps, SVG, or XML exports from user-supplied content can have trusted fields forged or overridden. Applications that never place untrusted text in a CDATA node are not affected. This issue affects saxy: from 0.7.0 before 1.7.0.	N/A	More Details
CVE-2026-66295	Saxy's XML encoder writes the target and the content of a processing instruction into the output document verbatim, without validation or escaping. The encoder builds the construct by concatenating both fields between <? and ?>, so neither field is checked against the constraints the XML specification places on it. Because ?> terminates a processing instruction, a target or content value containing that sequence closes the construct at a position the attacker chooses. Everything the attacker writes after it is emitted as ordinary markup at document level, which allows arbitrary elements, attributes, and further processing instructions to be injected into the serialized document. Appending a matching <? keeps the encoder's own terminator well-formed, so the result still parses and the injection is silent rather than a visible corruption. The target is additionally unconstrained by the XML Name production, which permits injection before the remainder of the processing instruction. The result is XML injection into a serialized document: the tree the application asks Saxy to encode and the tree a downstream parser reads back are no longer the same. Character data, attribute values, and comments are all escaped by the encoder, so processing instructions are the one construct that passes user bytes through untouched. Since Saxy.XML.processing_instruction/2 is a documented public builder, an application inherits the flaw without misusing the API. The consequences depend on what consumes the XML: forged records in a feed or export read by another system, injected stylesheet or rendering directives, or active content where the output is served to a browser as XML or SVG. This issue affects saxy: from 0.7.0 before 1.7.0.	N/A	More Details
CVE-2026-84155	CodeChecker's web server fails to fully invalidate a session token on logout when the server runs with more than one API worker process (the default). Each worker process maintains its own in-memory session cache; logout only clears the cache of the single worker that handles the request (plus the shared database record). Other workers continue to honor the destroyed token from their stale in-memory copies until the session's lifetime expires. An attacker who has captured a valid token can therefore keep impersonating the user after the user has logged out.	N/A	More Details
	The HTML report that plist-to-html, CodeChecker parse --export html and CodeChecker cmd diff --output html generate puts the report message, the checker name and the source file path into a script block through		

CVE-2026-84164	json.dumps. json.dumps does not escape the less-than character, so a closing script tag in any of those three fields ends the script element and what follows is parsed as HTML. The input author is whoever controls the analysed tree or a third-party result file that report-converter ingests, or who holds PRODUCT_STORE in the cmd diff flow. The viewer is somebody else: docs/jenkins_gerrit_integration.md documents writing the report into Jenkins userContent and posting its URL into a Gerrit review. One caveat worth stating up front is that Jenkins serves userContent under a restrictive CSP that would block an inline handler, so that destination is probably safe as configured. The generated report sets no CSP of its own, so the impact lands wherever it is published without one.	N/A	More Details
CVE-2025-66621	Apache James SASL OAuthBearer/XOAUTH2 prior versions 3.9.1 fails to validate correctly AUD claim of JWT payloads when introspection is not configured. This allows an attacker with valid credentials to access the mail server even if they are not authorized to do so. We recommend users to upgrade to non vulnerable version that forces explicit configuration of aud claims and forces introspection.	N/A	More Details
CVE-2026-85111	Allocation of Resources Without Limits or Throttling in Apache James Mime4J library prior version 0.8.15 allows Denial of Service upon parsing Mime messages. Users are recommended to upgrade to Apache James server 3.9.1 that relies on fixed MIME4J 0.8.15 which addresses the issue. See CVE-2026-85108 in Apache James MIME4J library.	N/A	More Details
CVE-2026-123746	The Symfony Security HTTP component AuthenticatorManager::authenticateUser() does not run the firewall user checker's checkPostAuth() method when a user is authenticated programmatically, allowing an account rejected by a custom user checker, such as an expired account, to be authenticated in Symfony versions prior to 5.4.56, 6.x prior to 6.4.50, 7.x prior to 7.4.23, and 8.x prior to 8.1.11. AuthenticatorManager::authenticateUser() is used by UserAuthenticatorInterface::authenticateUser() and by the SecurityBundle's Security::login() to authenticate a user programmatically, but it does not dispatch the security.authentication.success event, on which checkPostAuth() runs. The fix for CVE-2024-50341 made Security::login() call checkPreAuth(), but checkPostAuth() was still skipped. As a result, an account rejected by a custom user checker in checkPostAuth() is refused by form login and the other authenticators of the firewall, but can still be authenticated programmatically. Applications are affected when they use a custom user checker that rejects users in checkPostAuth() and authenticate users programmatically, for example after a password reset or an e-mail verification link. A user whose account is rejected can then obtain an authenticated session through that flow. The default user checker does nothing in checkPostAuth(), so the default configuration is not affected. The fix makes AuthenticatorManager::authenticateUser() dispatch the security.authentication.success event once the token is created and before it is stored, as authentications through the firewall do, so that checkPostAuth() runs and can reject the user.	N/A	More Details
CVE-2026-106019	Insertion of sensitive information into log file vulnerability in Johnson Controls C-CURE 9000, Victor allows Use of Known Operating System Credentials. This issue affects C-CURE 9000, Victor: 3.20.	N/A	More Details
CVE-2026-106020	Improper neutralization of input used for LLM prompting vulnerability in Johnson Controls EasyIO Neo IO Manager and Tools Installer allows Search Order Hijacking. This issue affects EasyIO Neo IO Manager and Tools Installer: 1.1.0.0.	N/A	More Details
CVE-2026-106022	Cleartext storage of sensitive information in memory vulnerability in Johnson Controls EasyIO Neo IOManager and Tools Installer allows Retrieve Embedded Sensitive Data. This issue affects EasyIO Neo IOManager and Tools Installer: 1.1.0.0.	N/A	More Details
CVE-2026-113618	The ZSIRep client library (ZSIREP.CLIENT.DLL) is vulnerable to improper server certificate validation. It registers a process-wide .NET callback that accepts any certificate for HTTPS connections without verification. This allows a man-in-the-middle attacker to impersonate the ZSIRep server and intercept or modify authentication data and documents. The callback persists after the client is closed, weakening other HTTPS connections in the same application. The issue was fixed in version 2.12.3.1. The library is used in KS-SOMED (fixed in 2026.03.0.01), KS-PPS (fixed in 2026.03.1.0), KS-MEDIS (fixed in 2026.03.0.0), KS-SOLAB (fixed in 2026.3.1.0), and KS-ASW (fixed in 2026.3.0.1).	N/A	More Details
CVE-2026-118514	In Symfony http-foundation prior to versions 5.4.56, 6.4.50, 7.4.23, and 8.1.11, Symfony\Component\HttpFoundation\RequestMatcher, and RequestMatcher\MethodRequestMatcher which replaces it from 6.2.x on, matches a request against a list of HTTP methods. These compared the request method to the list verbatim, while the router serves a HEAD request with the GET handler, as HTTP semantics require. This came after the incomplete fix of CVE-2026-45075 https://github.com/advisories/GHSA-6439-2f28-8p8q , which addressed the same gap in the #[IsGranted], #[IsSignatureValid] and #[IsCsrfTokenValid] attributes only. Security rules configured to apply only to GET requests could therefore be bypassed by sending a HEAD request to the same URL. Although HEAD responses contain no body, attackers could still access response headers and trigger the controller's execution, including any side effects. This issue also affects firewalls configured with methods: [GET]. A HEAD request would not match that firewall and could instead be handled by another matching firewall or no firewall at all. Applications using these vulnerable request matchers directly, including through a custom firewall request_matcher, could also be affected. The issue affects symfony/http-foundation through v5.4.55, v6.x through 6.4.49, v7.x through v7.4.22, and v8.x through v8.1.10.	N/A	More Details
CVE-2026-119170	There was a regression in how FIPS algorithms were enforced for the hashlib module. Only users that are using OpenSSL in FIPS mode are affected. Only Python 3.14.10 is affected, all other Python versions are unaffected.	N/A	More Details

CVE-2023-44363	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2023-44354	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2023-44349	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-34240	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-35680	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-35681	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-35682	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-35683	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-35684	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-35685	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-35686	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-35687	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-35688	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-42347	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-42353	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-42355	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-42358	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-42359	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-42361	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details

CVE-2022-42363	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-42368	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44464	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44472	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44475	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44476	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44477	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44478	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-35679	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-24100	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2023-38202	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-24088	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29118	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29119	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29120	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29121	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29122	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29123	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2020-29124	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details

CVE-2020-9619	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2021-21097	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2021-35998	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2021-39848	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2021-40704	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2021-40705	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2021-40706	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2021-40707	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2021-40717	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2021-45065	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2021-45066	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2021-45069	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2021-45070	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2021-46819	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-1060	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-24087	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44479	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44480	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44481	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details

CVE-2022-44482	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44524	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44525	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44526	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44527	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44528	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44529	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44530	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44531	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2023-21580	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2023-21600	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2023-21602	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2023-21617	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2023-21623	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2023-22245	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2023-22255	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2023-22267	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2023-22270	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2023-26357	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details

CVE-2023-26362	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2023-26363	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2023-26365	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2023-26399	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2023-29493	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44523	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44522	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44521	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44494	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44483	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44484	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44485	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44486	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44487	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44489	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44490	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44491	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44492	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44493	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details

CVE-2022-44495	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44511	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44496	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44497	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44501	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44503	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44504	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44505	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44506	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44507	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44508	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2022-44509	Rejected reason: Reserved ID never published and not linked to any VULN ticket - quota reclaim 2026-11-05	N/A	More Details
CVE-2026-99275	In the Linux kernel, the following vulnerability has been resolved: smb: client: reject short SESSION_SETUP responses smb2_check_message() accepts frames shorter than struct smb2_pdu when the SMB2 status is non-zero, before the minimum-PDU check added by b4694f269e66d. A 64-byte STATUS_MORE_PROCESSING_REQUIRED SESSION_SETUP response is therefore accepted even though it cannot contain the SecurityBufferOffset and SecurityBufferLength fields. The parser then reads those fields from stale bytes left in the reused receive buffer by an earlier frame. With a long stale SecurityBufferLength, decode_ntlmssp_challenge() copies up to about 64 KB from beyond the receive object and sends the data back to the server in the NTLMv2 AUTHENTICATE target info. Reject short MPR SESSION_SETUP responses before the short-error path, and validate SecurityBufferOffset + SecurityBufferLength against the received response length before decoding the challenge. The ordering bypass is not new: the short-error early return predates b4694f269e66d, and the unvalidated SecurityBufferLength read predates the 2016 raw NTLMSSP split in 166cea4dc3a4, so all supported stable trees are affected. Reproduced on 6.6.87.2; the path is unchanged on mainline.	N/A	More Details