SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 04 November 2026

Generated on 04 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-2026-61567	AVideo is a video-sharing Platform. Prior to 8.1.0, the live-streaming endpoint `view/videosListToLive.php` accepts an attacker-named streamer in `webSiteRootURL`, calls `Login::run` in `objects/Login.php`, and trusts the returned JSON as session state. An unauthenticated remote attacker who can host an HTTP service reachable by the encoder can self-grant `isLogged` and `canStream` without legitimate credentials. The endpoint requires only nonempty `playlists_id` and `APISecret` values; `APISecret` is forwarded rather than checked against a stored secret. This path never calls `Streamer::isURLAllowed` and therefore works regardless of the operator's streamer allowlist. It fetches a second attacker-controlled video-list response and interpolates `videos[].path` without shell argument escaping into `ffprobe` and `ffmpeg` commands passed to `exec`; `isAudio` calls `isVideo` to reach the `ffprobe` command. Paths containing shell delimiters execute arbitrary operating-system commands as the web-server user. The request filter does not inspect the video-list JSON. This can disclose database and stored streamer credentials, compromise the upstream platform using those credentials, modify files owned by the web-server user, establish persistence, and deny encoder service. This issue is fixed in version 8.1.0.	10.0	More Details
CVE-2026-61564	AVideo is a video-sharing Platform. Prior to 8.1.0, the unauthenticated installer endpoint `install/checkConfiguration.php` assembles `videos/configuration.php` by interpolating request parameters, including `webSiteRootURL`, into single-quoted PHP string literals without escaping. An attacker can terminate a literal and inject PHP that executes as the web-server user when the generated, directly requestable file is loaded. Exploitation requires `videos/configuration.php` to be absent, as on every fresh deployment or after the file is removed or moved; an existing file blocks this endpoint. The supplied `systemRootPath` must contain index.php and a connection using `databaseHost`, `databaseUser`, and `databasePass` must succeed, but the attacker can point those parameters to their own database server and needs no target credentials. The write location is also derived from `systemRootPath` without a base-directory constraint. This permits arbitrary command execution, reading and overwriting files owned by the web-server user, persistent PHP code, and control over stored database connection settings. The endpoint additionally interpolates request values into streamer and configuration INSERT statements, creating a secondary SQL-injection sink. This issue is fixed in version 8.1.0.	10.0	More Details
CVE-2026-61991	Unauthenticated Remote Code Execution (RCE) in AjaxLoadMore Cache <= 3.1.1 versions.	10.0	More Details
CVE-2026-84295	Improper authentication in Progress Software WS_FTP Server versions prior to 2024.0.6 and 2025.0.3 on Windows could allow an unauthenticated remote attacker to access sensitive information, including administrative credentials.	10.0	More Details
CVE-2026-61738	SOCFortress CoPilot focuses on providing a single pane of glass for all your security operations needs. Prior to 0.1.77, `POST /api/scoutsuite/generate-gcp-report` in `backend/app/integrations/scoutsuite/routes/scoutsuite.py` admits admin and analyst users and validates the uploaded content as `GCPScoutSuiteJSON`, but passes raw `file.filename` from the multipart header to `save_file_to_directory` in `backend/app/integrations/scoutsuite/services/scoutsuite.py`. The writer combines this filename with `scoutsuite-report` using `os.path.join` without sanitization or a resolved-path containment check. A traversal filename therefore writes the supplied JSON outside the intended report directory. In the reported root-running backend, the researcher demonstrated root-owned writes outside that directory and into the application source directory. This permits host-file overwrite subject to the accepted JSON-content constraint and can disrupt application operation; the demonstrated primitive does not establish unrestricted executable contents or unconditional cross-tenant confidentiality loss. Version 0.1.77 removes caller-controlled filenames from the affected route; unrestricted-content and direct-code-execution claims require separate curator reconciliation.	10.0	More Details
CVE-2026-61826	Bazarr is a companion application to Sonarr and Radarr. Prior to 1.5.7-beta.14, the `api_ns_plex` namespace in `bazarr/api/plex/oauth.py` omits `@authenticate` on its Resource handlers, while normal APIs require an API key and no global authentication hook compensates. Anonymous callers can invoke `POST /api/plex/oauth/logout` to clear credentials and disable the integration, or `POST /api/plex/apikey` to persist an attacker-selected key, without a PIN, account or state precondition. `POST /api/plex/oauth/pin` and `GET /api/plex/oauth/pin/<pin_id>/check` additionally allow an attacker who completes a PIN with an attacker-controlled Plex account to bind that account's token to the instance. `PlexPinCheck` skips state validation when `state_param` is absent and merely logs a mismatch without stopping execution. `POST /api/plex/select-server`, `POST /api/plex/oauth/servers`, `POST /api/plex/webhook/create`, `POST /api/plex/webhook/delete` and `POST /api/plex/encrypt-	10.0	More Details

	apikey` expose further `write_config()` operations. Attacker-controlled server URLs feed later outbound requests carrying the configured API key in `X-Plex-Token`, enabling server-side request forgery and credential exposure in addition to persistent configuration tampering and integration denial of service. Version 1.5.7-beta.14 closes the anonymous API-mutation path by adding authentication; complete OAuth state validation is not established and remains a separate residual for curator review.		
CVE-2026-61728	SOCFortress CoPilot focuses on providing a single pane of glass for all your security operations needs. In affected snapshots preceding the respective 0.1.70 and 0.1.76 sink repairs, portal users, including `customer_user`, can submit stored markup through `POST /api/incidents/db_operations/alert/comment`. In `customer-portal/src/components/alerts/AlertDetails/AlertComment.vue`, `commentHtml` replaces newlines in `comment.comment` but passes the result to `v-html` without escaping or sanitizing HTML. When another user views the poisoned alert, stored script executes on the application origin; the same unsanitized rendering pattern affects server-stored SOC case, asset and health-check fields in `SocCaseNote.vue`, `SocCaseItem.vue`, `SocCaseAssetsItem.vue`, `SocAlertAssetsItem.vue` and `HealthcheckItem.vue`. The authentication store in `customer-portal/src/stores/auth.ts` persists both access and refresh tokens in JavaScript-readable storage, and `customer-portal/src/api/httpClient.ts` uses bearer headers rather than HttpOnly cookies. An injected script can steal both tokens, impersonate the viewer and obtain fresh tokens through `/auth/refresh`. If an analyst or administrator views the poisoned alert or case, this enables persistent privileged account takeover, cross-tenant data access, incident modification or deletion, and detection/response subversion. The health-check sink repair is first contained in version 0.1.70, while the comment and other SOC sink repairs are first contained in version 0.1.76. Version 0.1.76 is the provisional first release containing all observed repairs; grouped versus split CVE scope requires curator adjudication.	9.9	More Details
CVE-2026-107327	IBM Langflow OSS 1.0.0 through 1.12.4 could allow a remote authenticated attacker to execute arbitrary code due to missing authorization.	9.9	More Details
CVE-2026-107328	IBM Langflow OSS 1.0.0 through 1.12.4 could allow a remote authenticated attacker to execute arbitrary code due to improper neutralization of code in eval/exec.	9.9	More Details
CVE-2026-44179	XWiki Remote Macros provides XWiki rendering macros that are useful when migrating content from Confluence. From 1.13 until 1.14.5, the `excerpt-include` macro does not properly escape the included page's title and executes `excerpt` content with the macro's rights. The title handling in `xwiki-pro-macros-ui/src/main/resources/Confluence/Macros/ExcerptInclude.xml` and the rendering of `excerpt` content into XWiki syntax both allow syntax injection. Any user able to edit a page, even without script or programming rights, can supply executable macro syntax in the title or `excerpt` and cause remote code execution when the page is included. This affects confidentiality, integrity and availability of the whole XWiki installation. This issue is fixed in version 1.14.5.	9.9	More Details
CVE-2026-119145	Frappe before 15.121.0 and 16.x before 16.34.0 contains a path traversal vulnerability because certain file-upload handling does not validate the destination path before writing to disk. Authenticated attackers can upload crafted files to locations outside the intended storage directory to achieve remote code execution on the server.	9.9	More Details
CVE-2026-90868	An OS command injection vulnerability in Progress Software WS_FTP Server versions prior to 2024.0.7 and 2025.0.4 on Windows could allow arbitrary command execution under certain configurations.	9.9	More Details
CVE-2026-116241	pgAdmin 4's Import/Export Data tool wraps a user's query export in a psql \copy (...) TO command and checks that the query's parentheses are balanced so that nothing can escape the wrapper. The check rejected a backslash inside a single-quoted string, but not inside a double-quoted identifier, where it treated the next double quote as closing the identifier. psql's \copy parser applies the connection's escape character to whichever quote opened a token, so with standard_conforming_strings off a backslash-escaped double quote does not close the identifier. pgAdmin's and psql's view of the quoting then diverged, a closing parenthesis hidden from the check ended the \copy (...) wrapper, and a following TO PROGRAM clause was executed by psql on the pgAdmin host, as the operating-system account running pgAdmin, before the server rejected the statement. An ordinary database role can turn standard_conforming_strings off for itself, and the Import/Export Data permission is granted to non-administrators by default. This is a bypass of the fix for CVE-2026-17566. The fix rejects any backslash inside a double-quoted identifier, as was already done for single-quoted strings, since its meaning depends on a server setting that cannot be known reliably when the query is validated. This issue affects pgAdmin 4: before 9.19.	9.9	More Details
CVE-2026-113617	The Automated Import Products to Cart WordPress plugin before 1.0.4 does not sanitize a user-supplied file path before using it to read and delete files, allowing users with minimal permissions, such as subscribers, to read arbitrary files (including ones containing the database credentials) and delete arbitrary files on the server.	9.9	More Details
CVE-2026-62853	ThingLinks is an enterprise IoT platform. Prior to 1.4.0, the `/groovyScriptTest/registerScript` endpoint accepts user-supplied Groovy script content and passes it to an unsandboxed `Groovy compilation and loading` flow. An authenticated attacker can provide code that is compiled and instantiated on the server, resulting in arbitrary server-side code execution. The issue affects the `rule engine`'s Groovy script test/register flow. This issue is fixed in version 1.4.0.	9.9	More Details
CVE-2026-107329	IBM Langflow OSS 1.0.0 through 1.12.4 could allow a remote authenticated attacker to execute arbitrary code due to improper control of code generation.	9.9	More Details
CVE-2026-62013	Unauthenticated PHP Object Injection in Edge Decor <= 2.9 versions.	9.8	More Details
CVE-2026-62014	Unauthenticated PHP Object Injection in EmojiNation <= 1.0.12 versions.	9.8	More Details
CVE-2026-110879	jackson-databind validates the outer class of a class-name type ID but accepts attacker-selected classes inside its generic arguments, even when those classes violate the declared type or would be rejected as direct type IDs. This bypasses the generic-argument validation added for CVE-2026-54512 (GHSA-j3rv-43j4-c7qm), of which this is an incomplete fix. DatabindContext._resolveAndValidateGeneric() checks the outer class against the declared base type and then passes each argument from the type ID to _validateTypeParameter(), which validates the argument against the outer base type rather than enforcing its corresponding declared generic binding. It also invokes validators with arguments that have not passed the subtype check those validators expect. Under the default DefaultBaseTypeLimitingValidator this accepts an unrelated class inside a generic subtype even when the same class is rejected as a direct type ID. Where an allowIfBaseType(...) rule approves the outer type, Jackson substitutes LaissezFaireSubTypeValidator, so the configured validator no longer restricts the embedded arguments. The element type of a plain array type ID such as [Lpkg.Gadget; is likewise left unvalidated once the array's base type is approved. Affected paths include annotation-based class-name polymorphism with a default Jackson 3.x JsonMapper, configured default typing in both Jackson 2.x and 3.x, and integrations that expose that default typing. The default-validator case requires no application-authored validator: with @JsonTypeInfo(use = Id.CLASS), a direct gadget type ID is rejected as "Not a subtype", while a type ID naming a generic wrapper around the same gadget is accepted and deserialized, including attacker-supplied bean properties. Where class-name default typing permits Map, a property declared as Map<String,String> accepts	9.8	More Details

	HashMap<FileSystemXmlApplicationContext,String>; map-key discovery then passes the attacker-controlled JSON property name to the selected class's one-string constructor. With Spring on the classpath and attacker-controlled XML the application can load, that constructor loads the XML and invokes ProcessBuilder.start() under the application account, giving arbitrary command execution. This issue affects com.fasterxml.jackson.core:jackson-databind from 2.10.0 and tools.jackson.core:jackson-databind from 3.0.0. Releases before 2.10.0 are not affected, because PolymorphicTypeValidator was introduced in jackson-databind 2.10.0.		
CVE-2026-62015	Unauthenticated PHP Object Injection in Gamezone <= 1.1.11 versions.	9.8	More Details
CVE-2026-62011	Unauthenticated PHP Object Injection in Bonbon <= 1.11 versions.	9.8	More Details
CVE-2026-62016	Unauthenticated PHP Object Injection in Gamic <= 1.19 versions.	9.8	More Details
CVE-2026-62012	Unauthenticated PHP Object Injection in Coinpress <= 1.0.15 versions.	9.8	More Details
CVE-2026-62006	Unauthenticated PHP Object Injection in Nuts <= 1.12 versions.	9.8	More Details
CVE-2026-62010	Unauthenticated PHP Object Injection in Avventure <= 1.1.12 versions.	9.8	More Details
CVE-2026-62009	Unauthenticated PHP Object Injection in Filmax <= 1.1.11 versions.	9.8	More Details
CVE-2026-62008	Unauthenticated PHP Object Injection in Orpheus <= 1.8 versions.	9.8	More Details
CVE-2026-62018	Unauthenticated PHP Object Injection in Gunslinger <= 1.11 versions.	9.8	More Details
CVE-2026-62005	Unauthenticated PHP Object Injection in Muzicon <= 1.15 versions.	9.8	More Details
CVE-2026-106013	The Jupiter X Core plugin for WordPress is vulnerable to Authentication Bypass via the Twitter/X Social Login handler in all versions up to and including 4.61.0. The vulnerability exists within the verify_twitter_callback function because after exchanging the visitor's oauth_verifier for their access token, the handler never calls setOauthToken() to reassign the returned credentials to the TwitterOAuth client, causing the subsequent account/verify_credentials API call to remain signed with the site operator's stored Access Token and Access Token Secret rather than the authenticating visitor's token. This causes the X API to return the profile of the X application owner instead of the signing-in visitor, and the plugin then resolves and authenticates a WordPress account solely by matching that owner's email address via wp_set_auth_cookie(), allowing unauthenticated attackers to gain authenticated access as the WordPress user whose email corresponds to the X app owner, who is typically the site administrator.	9.8	More Details
CVE-2026-62003	Unauthenticated PHP Object Injection in Mission <= 1.22 versions.	9.8	More Details
CVE-2026-62002	Unauthenticated PHP Object Injection in Meals & Wheels <= 1.1.13 versions.	9.8	More Details
CVE-2026-62001	Unauthenticated PHP Object Injection in Marcell <= 1.2.14 versions.	9.8	More Details
CVE-2026-61998	Unauthenticated PHP Object Injection in Le Truffe <= 1.1.7 versions.	9.8	More Details
CVE-2026-61997	Unauthenticated PHP Object Injection in Legal Stone <= 1.2.11 versions.	9.8	More Details
CVE-2026-62017	Unauthenticated PHP Object Injection in Good Homes <= 1.3.13 versions.	9.8	More Details
CVE-2026-107048	An issue in the WebView rendering path component of MotionCreative Motion UI versionCode 101 allows attackers to execute arbitrary code via supplying a crafted POST request.	9.8	More Details
CVE-2026-62131	Unauthenticated PHP Object Injection in Zoho Flow <= 2.14.5 versions.	9.8	More Details
CVE-2026-119660	MuseBot before 2.0.0 contains an authentication bypass vulnerability that allows unauthenticated attackers to forge admin sessions by using the hard-coded default session_key 'muse_bot_session_key'. Attackers can sign a MuseBot-session cookie carrying a user_id to gain full administrative access, reading password hashes, chat records, and bot configuration, and stopping bots.	9.8	More Details
CVE-2026-78403	Stack-based buffer overflow and missing authorization vulnerability in Thales Sentinel Keys Server on Windows allows Overflow Buffers. Sentinel Keys Server does not check the length of the first field in the HTTP request. An attacker may craft an HTTP request and send it to Sentinel Keys Server. It may lead to remote code execution as NT AUTHORITY\SYSTEM. This issue affects Sentinel Keys Server: versions lower than 1.3.8.0.	9.8	More Details
CVE-2026-61620	HoneySQL turns Clojure data structures into SQL. From 2.0.0 until 2.7.1392, applications that pass user input or other arbitrary data into the HoneySQL `DSL` by calling `keyword` or `symbol` on that input can produce SQL strings that facilitate SQL injection when executed unchanged by a `JDBC` driver. Some formatters do not apply the existing suspicious-character check to the resulting entity names. The impact depends on the privileges of the database connection executing the generated statement. Input validation before constructing `keyword` or `symbol` entities is a workaround. The maintainer-designated fixed version is 2.7.1392.	9.8	More Details

CVE-2026-90888	Unauthenticated PHP Object Injection in LeadSnap <= 1.25 versions.	9.8	More Details
CVE-2026-39738	Deserialization of Untrusted Data vulnerability in Aman FunnelKit Automations wp-marketing-automations allows Object Injection.This issue affects FunnelKit Automations: from n/a through 3.8.6.1.	9.8	More Details
CVE-2026-119526	Deserialization of Untrusted Data vulnerability in ThemeREX Royal Event allows Object Injection. This issue affects Royal Event: from n/a through 2.0.	9.8	More Details
CVE-2026-116386	Unauthenticated Privilege Escalation in SMS Alert Order Notifications <= 4.0.2 versions.	9.8	More Details
CVE-2026-119716	pybars3 through 0.9.7 and pybars4 through 0.9.13 contain a code injection vulnerability in pybars/_compiler.py that allows template authors to execute Python code via unescaped bracketed path segments. Attackers can supply Handlebars templates with crafted segments in helper or block arguments to break out of string literals and execute Python in the application process.	9.8	More Details
CVE-2026-119706	InternLM LMDeploy 0.9.0 through 0.18.0 contains an unauthenticated remote code execution vulnerability that allows remote attackers to run OS commands by sending pickled data to the /update_weights endpoint. Attackers can submit a base64-encoded crafted pickle in serialized_named_tensors, which ForkingPickler.loads deserializes without validation, executing commands as the api_server process.	9.8	More Details
CVE-2026-61737	ng-antd-admin is an Angular and NestJS administration system template. Prior to 22.0, a hardcoded default `JWT` secret permits token forgery when a deployment has not replaced the default secret, without a startup warning. An attacker can bypass authentication and authorization, impersonate any user including administrators, and access protected API endpoints, leading to account takeover, data leakage and unauthorized operations. Version 22.0 rejects the shipped secret in production but permits it with a warning in non-production environments.	9.8	More Details
CVE-2026-110799	Vvveb is a powerful and easy to use CMS with page builder to build websites, blogs or ecommerce stores. Prior to version 1.0.8.7, the password reset functionality is vulnerable to an Authentication Bypass due to insufficient validation of the user and token GET parameters. This issue has been patched in version 1.0.8.7.	9.8	More Details
CVE-2026-93680	IBM Langflow OSS 1.0.0 through 1.12.8 could allow a remote attacker to bypass security restrictions due to improper authentication.	9.8	More Details
CVE-2026-119597	OpenDeepWiki through 2.0.6 contains a hard-coded JWT signing key vulnerability that allows unauthenticated attackers to forge administrator tokens using the publicly known Jwt:SecretKey in appsettings.json. Attackers can mint HS256 bearer tokens with an Admin role claim to access /api/admin endpoints and control users, roles, repositories, settings, and API keys.	9.8	More Details
CVE-2025-31704	A vulnerability has been found in the Dahua Intelligent Connection Center. A remote attacker could send a specially crafted request to the affected system, allowing the attacker to execute arbitrary commands, resulting in remote code execution.	9.8	More Details
CVE-2026-64618	Improper Neutralization of Special Elements used in an SQL Command ("SQL Injection") vulnerability exists in Apache Fineract (through version 1.15.0). The vulnerability affects the outStandingAmountPercentageCondition parameter of the /fineract-provider/api/v1/search/advance HTTP API endpoint, allowing SQL injection due to insufficient input neutralization. Users are recommended to upgrade to version 1.16.1, which will fix the issue.	9.8	More Details
CVE-2026-103039	The Gravity Forms plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 3.1.2 via a Post Custom Field whose input type is List. This is due to GFFormsModel::create_post() passing the submitted value to WordPress' unrestricted global maybe_unserialize() rather than the plugin's own hardened GFCommon::maybe_unserialize(), which was added in 3.1.1 and passes allowed_classes => false precisely to prevent object instantiation. Where the field has a content template enabled, the submitted row reaches that call verbatim. This makes it possible for unauthenticated attackers to inject a PHP object into post meta. No PHP Object Injection gadget chain is present in the plugin itself; however, if a gadget chain is present via an additional plugin or theme, it could allow the attacker to perform actions such as remote code execution. Where the custom field is mapped to the protected _wp_page_template meta key, WordPress itself supplies the chain: validate_file() accepts non-scalars, WP_Theme::__toString() then resolves an attacker-controlled path, and on hosts with a readable PEAR install and register_argc_argv enabled this yields remote code execution.	9.8	More Details
CVE-2026-107249	Improperly Controlled Modification of Dynamically-Determined Object Attributes vulnerability in Drupal Block AJAX allows Object Injection. This issue affects Block AJAX versions: from 0.0.0 to 3.0.2.	9.8	More Details
CVE-2026-51912	OpenBMB XAgent v1.0.0 contains directory traversal vulnerability in main-upload_file-the-preserved-live-upload-file-witness-directly-reaches (ToolServer/ToolServerNode/main.py:46).	9.8	More Details
CVE-2026-107058	An issue in Shelter versionCode 445 allows attackers to register their own auth_key and execute a takeover of another user's binder service API and preference state.	9.8	More Details
CVE-2026-107057	An issue in AndBible versionCode 1111 allows attackers to execute arbitrary code via uploading a crafted module zip.	9.8	More Details
CVE-2026-107050	An issue in libretro RetroArch v1.22.2 allows attackers to force another user into loading attacker-supplied code in their uid, leading to arbitrary code execution.	9.8	More Details
CVE-2026-61992	Unauthenticated PHP Object Injection in GEO my WordPress <= 4.5.5.3 versions.	9.8	More Details
CVE-2026-62004	Unauthenticated PHP Object Injection in Motorix <= 1.11 versions.	9.8	More Details
CVE-2026-54860	Unauthenticated PHP Object Injection in Ozisti <= 1.1.10 versions.	9.8	More Details
	In the Linux kernel, the following vulnerability has been resolved: scsi: libiscsi: Validate the ITT reflected in a Reject PDU A Reject PDU carries a copy of the header it rejects, and iscsi_handle_reject() takes the ITT out of that copy to find the task to clean up: memcpy(&rejected_pdu, data, sizeof(struct iscsi_hdr)); ... task = iscsi_itt_to_task(conn, rejected_pdu.itt); That value is whatever the target put there. iscsi_itt_to_task() bounds the index against cmds_max and checks nothing else, so any task in the pool can be named, and iscsi_nop_out_rsp() then completes it. An index that has never been used gives a NULL task->conn: the pool is zeroed at session setup and conn is assigned only when a task is allocated. If the task was used and returned, iscsi_complete_task() hits its WARN_ON_ONCE(task->state == ISCSI_TASK_FREE) and the refcount underflows. An in-flight SCSI command is completed as successful - a 1 MiB read returned 1048576 with none of its buffer written and no warning. Validate		

CVE-2026-99153	the reflected ITT the way iscsi_itt_to_ctask() validates a command ITT, and require the task to be in flight and not a SCSI command. [6.248477] Oops: general protection fault, probably for non-canonical address 0xdffffc000000000c: 0000 [#1] SMP KASAN NOPTI [6.249357] KASAN: null-ptr-deref in range [0x0000000000000060-0x0000000000000067] [6.249951] CPU: 1 UID: 0 PID: 0 Comm: swapper/1 Not tainted 7.2.0-rc5-ISCSI1-gf5098b6bae76 #1 PREEMPT(lazy) [6.250718] Hardware name: QEMU Ubuntu 24.04 PC v2 (i440FX + PIIX, arch_caps fix, 1996), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 [6.251616] RIP: 0010:iscsi_nop_out_rsp.constprop.0+0x46/0x160 [6.252043] Code: c1 ea 03 48 83 ec 08 80 3c 02 00 0f 85 f5 00 00 00 48 b8 00 00 00 00 00 fc ff df 48 8b 6b 58 48 8d 7d 60 48 89 fa 48 c1 ea 03 <80> 3c 02 00 0f 85 c0 00 00 00 48 8b 45 60 48 39 c3 74 50 48 b8 00 [6.252813] RSP: 0018:ffff88806c907b80 EFLAGS: 00010206 [6.253042] RAX: dfffc0000000000 RBX: ffff88800607e000 RCX: ffffffff8d571a25 [6.253345] RDX: 000000000000000c RSI: ffff88806c907c38 RDI: 0000000000000060 [6.253642] RBP: 0000000000000000 R08: 0000000000000000 R09: fffffbfff235a504 [6.253947] R10: 0000000000000003 R11: 7463656e6e6f6320 R12: 0000000000000000 [6.254251] R13: 0000000000000000 R14: ffff88806c907c38 R15: 0000000000000000 [6.254549] FS: 0000000000000000(0000) GS:ffff8880d95bc000(0000) knlGS:0000000000000000 [6.254887] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [6.255140] CR2: 00007fc393e8ffc0 CR3: 0000000005252006 CR4: 0000000000770ef0 [6.255439] PKRU: 55555554 [6.255564] Call Trace: [6.255674] <IRQ> [6.255768] __iscsi_complete_pdu+0x18bf/0x22a0 [6.256733] iscsi_complete_pdu+0x54/0xa0 [6.256905] iscsi_tcp_data_recv_done+0xf4/0x250 [6.257103] iscsi_tcp_recv_skb+0x31e/0xec0 [6.257680] iscsi_sw_tcp_recv+0x12f/0x390 [6.258061] __tcp_read_sock+0x1ab/0x810 [6.258853] iscsi_sw_tcp_data_ready+0x18b/0x510 [6.259808] tcp_data_queue+0x1f13/0x4cd0 [6.260567] tcp_rcv_established+0x8a5/0x3a00 [6.261931] tcp_v4_do_rcv+0x449/0x960 [6.262269] tcp_v4_rcv+0x2245/0x3bc0	9.8	More Details
CVE-2026-118579	A weakness has been identified in D-Link DIR-505 1.10B02. The impacted element is the function main of the file /secmark1524.cgi of the component Web Management CGI. This manipulation of the argument accu/pass/code/hash/cmds causes backdoor. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks.	9.8	More Details
CVE-2026-109516	The Bot for Telegram on WooCommerce plugin for WordPress is vulnerable to Authentication Bypass leading to Account Takeover in all versions up to, and including, 1.3.0. The `/wp-json/woo-telegram/v1/main/` REST endpoint is registered with `permission_callback => '__return_true'` and performs no Telegram webhook signature verification, allowing an unauthenticated attacker to POST a forged bot update with a `message.chat.id` set to any WordPress login name; `bftow_get_user_system_id()` resolves this attacker-supplied value to the targeted account via `get_user_by('login', $tgId)` with no ownership proof, and writes a login token computed as `md5($_SERVER['HTTP_USER_AGENT'] . time())` — both inputs are fully attacker-controlled or bounded within seconds using the response's own `Date` header. The resulting token is redeemable at the unauthenticated, capability-check-free, and nonce-less `?action=bftow_create_order&bftow_token=` endpoint, which calls `wp_set_auth_cookie()` unconditionally via `login_user_by_id`, issuing a persistent authenticated session cookie for the targeted account to the attacker. This makes it possible for unauthenticated attackers to log in as any WordPress user, including administrators, given only that user's username.	9.8	More Details
CVE-2026-42922	A authorization bypass vulnerability exists in the /nodered functionality of FUXA (version(s): 1.3.2-2809). A specially crafted HTTP request can lead to a arbitrary code execution. An attacker can make an unauthenticated HTTP request to trigger this vulnerability.	9.8	More Details
CVE-2026-103409	A Missing authentication for critical function vulnerability in Juniper Networks Session Smart Router allows an unauthenticated network-based attacker to obtain administrative privileges by passing crafted URL parameters to an insecure endpoint running as root. Note that this vulnerability can only be exploited prior to the device being onboarded to Mist/Conductor. The issue can no longer be exploited once a device is onboarded to Mist/Conductor.	9.8	More Details
CVE-2026-103406	An Improper Neutralization of Special Elements used in an OS Command vulnerability in the AutomatedProvisioner in Juniper Networks Session Smart Conductor allows a remote attacker to execute arbitrary commands as root via a specially crafted salt minion ID.	9.8	More Details
CVE-2026-115968	Deserialization of Untrusted Data vulnerability in Ultimate Member Ultimate Member ultimate-member allows Object Injection.This issue affects Ultimate Member: from n/a through 2.13.1.	9.8	More Details
CVE-2026-118477	The ei_git_repo_url parameter in the Git remote configuration endpoint of KaliFast is vulnerable to OS Command Injection. This OS Command Injection vulnerability allows an authenticated attacker (free registration available) to execute arbitrary commands on the KaliFast server with www-data privileges. Fixed in version 2026061802.	9.8	More Details
CVE-2026-113616	The LogixFast Auth WordPress plugin before 1.0.4 does not deliver its password-reset one-time code to the resolved account's own email address, mailing it to the address supplied in the request instead, allowing unauthenticated attackers to reset any user's password, including an administrator's, and take over the account.	9.8	More Details
CVE-2026-115245	The Chat AI with Dispatcher WordPress plugin before 2.4 does not properly validate uploaded files, relying only on a spoofable client-supplied content type, allowing unauthenticated attackers to upload arbitrary files, including PHP, which can lead to remote code execution.	9.8	More Details
CVE-2026-114278	The che-machine-exec service constructs a shell command by concatenating user-controlled input (the username and namespace fields from the /exec/init and /exec/config JSON endpoints) into a double-quoted sh -c "echo "..." > ..." invocation without any escaping. When che-machine-exec is run with authentication disabled (its default), any network-reachable attacker can achieve remote code execution in containers che-machine-exec is configured to access, via shell command substitution ($(...) or backticks).	9.8	More Details
CVE-2026-97854	Yamaha wireless LAN router NWR100 provided by Yamaha Corporation contains an OS command injection vulnerability. Arbitrary OS commands may be executed by sending a specially crafted request to the affected product.	9.8	More Details
CVE-2026-79589	The WIFI4 N300 router (Model: T1 Pro) v1.0.0 by U-speed contains an insecure access control flaw that allows an attacker to gain unauthenticated root shell. The vulnerability is caused by the exposure of the UART debugging interface having a lack of authentication, authorization and access control functionality. Once the interface is soldered and connected to the attacker, they gain root privilege to the system.	9.8	More Details
CVE-2026-118690	Signal K Server before 2.33.0 contains a missing authentication vulnerability that allows unauthenticated remote attackers to download log archives via the /skServer/ziplogs endpoint. Attackers can extract the JWT secretKey from security.json in the ZIP, forge administrator tokens, and create persistent admin accounts for full server control.	9.8	More Details
CVE-2026-	In the Linux kernel, the following vulnerability has been resolved: scsi: libiscsi: Reject a negative task index from parse_pdu_itt A transport that implements parse_pdu_itt hands libiscsi an index taken from the PDU, and both lookups bound it from above only: if (i >= session->cmds_max) i and cmds_max are both int, so a negative index passes and session->cmds[i] is read from before the array. be2iscsi produces one. beiscsi_parse_pdu() assigns the raw tag, *index = (int)itt; and beiscsi_complete_pdu()	9.8	More Details

99154	forwards an unsolicited NOP-In from the hardware async ring without replacing its ITT, so the value is the target's. It also reports the session's own age rather than the one in the tag, which leaves the age comparison in iscsi_verify_itt() with nothing to reject. Bound the index from below in both lookups.		
CVE-2026-103688	The Checkout Files Upload for WooCommerce WordPress plugin before 2.4.0 does not validate uploaded file types when its accepted file types setting is left empty, which it documents as the way to accept all files, allowing unauthenticated users to upload arbitrary files, including PHP files that lead to remote code execution on servers that execute PHP from the uploads directory.	9.8	More Details
CVE-2026-109218	The Contact Manager plugin for WordPress is vulnerable to Arbitrary File Upload in all versions up to, and including, 9.1.2 via the add_message function. This is due to an incomplete extension blacklist that fails to detect dangerous extensions when a trailing dot causes the extension-derivation routine to return an empty string, which sanitize_file_name() then silently removes before the file is written to disk. This makes it possible for unauthenticated attackers to upload files that may be executable, which makes remote code execution possible. Successful code execution additionally requires the server to use Apache with libapache2-mod-php (which maps .phar to PHP by default) and the attacker to retrieve the uploaded file within the brief window before it is removed by unlink() at end of request.	9.8	More Details
CVE-2026-54858	Unauthenticated PHP Object Injection in Printy <= 1.13.0 versions.	9.8	More Details
CVE-2026-54857	Unauthenticated PHP Object Injection in Quirky <= 1.23 versions.	9.8	More Details
CVE-2026-54856	Unauthenticated PHP Object Injection in RexCoin <= 1.2.6 versions.	9.8	More Details
CVE-2026-110186	IBM Langflow OSS 1.0.0 through 1.12.8 could allow a remote attacker to execute arbitrary code due to improper control of code generation.	9.8	More Details
CVE-2026-84999	The Pie Register Premium plugin for WordPress is vulnerable to Unrestricted File Type Upload in all versions up to, and including, 3.8.4.0 via the piereg_file_upload function. This is due to the plugin performing file type validation via wp_check_filetype and wp_check_filetype_and_ext but never checking whether those validation calls produced errors before move_uploaded_file() is called, combined with no nonce or capability check on the AJAX handler. This makes it possible for unauthenticated attackers to upload files of dangerous types (e.g. PHP scripts) that may be executable, which makes remote code execution possible. The server returns the generated destination filename in the response, giving the attacker the exact path needed to trigger the uploaded file.	9.8	More Details
CVE-2026-54859	Unauthenticated PHP Object Injection in Preservation <= 1.15 versions.	9.8	More Details
CVE-2026-86397	Dell PowerProtect Data Domain, Feature Release versions 7.7.1.0 through 8.8, LTS2024 release versions 7.13.1.0 through 7.13.1.80, LTS2025 release versions 8.3.1.0 through 8.3.1.40, LTS2026 release versions 8.6.1.0 through 8.6.1.20, contain an Improper Authentication vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to privileged account creation. This is a critical severity vulnerability as it allows an attacker to take complete control of the system. Dell recommends customers to upgrade at the earliest opportunity.	9.8	More Details
CVE-2026-86400	Dell PowerProtect Data Domain, Feature Release versions 7.7.1.0 through 8.8, LTS2024 release versions 7.13.1.0 through 7.13.1.80, LTS2025 release versions 8.3.1.0 through 8.3.1.40, LTS2026 release versions 8.6.1.0 through 8.6.1.20, contain an Improper Authentication vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges. This is a critical severity vulnerability as it allows an attacker to take complete control of the system. Dell recommends customers to upgrade at the earliest opportunity.	9.8	More Details
CVE-2026-86384	Dell PowerProtect Data Domain, Feature Release versions 7.7.1.0 through 8.8, LTS2024 release versions 7.13.1.0 through 7.13.1.80, LTS2025 release versions 8.3.1.0 through 8.3.1.40, LTS2026 release versions 8.6.1.0 through 8.6.1.20, contain an Use of Hard-coded Cryptographic Key vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to credential exposure. The credentials may be used to access the system with privileges of the compromised user.	9.8	More Details
CVE-2026-103780	Dell PowerProtect Data Domain, Feature Release versions 7.7.1.0 through 8.8, LTS2024 release versions 7.13.1.0 through 7.13.1.80, LTS2025 release versions 8.3.1.0 through 8.3.1.40, LTS2026 release versions 8.6.1.0 through 8.6.1.20, contain a Stack-based Buffer Overflow vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to command execution.	9.8	More Details
CVE-2026-104339	IBM Langflow OSS 1.0.0 through 1.12.3 could allow a remote attacker to execute arbitrary code due to improper neutralization of special elements used in an OS command.	9.8	More Details
CVE-2026-115904	Topluyo is a social networking platform. A vulnerability exists in Topluyo Desktop for Linux prior to version 2026.9.2410 where user-controlled URLs are unsafely processed, leading to OS Command Injection via the `openExternalLinks()` routine in `utils.js`. An attacker who controls a target URL can execute arbitrary operating system commands with the privileges of the user running the application upon opening the link. Version 2026.9.2410 patches the issue.	9.6	More Details
CVE-2026-103792	Dell PowerProtect Data Domain Management Center, Feature Release versions 7.7.1.0 through 8.8, LTS2024 release versions 7.13.1.0 through 7.13.1.80, LTS2025 release versions 8.3.1.0 through 8.3.1.40, LTS2026 release versions 8.6.1.0 through 8.6.1.20, contain an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Unauthorized access to managed systems.	9.6	More Details
CVE-2026-119263	Use after free in GarbageCollection in Google Chrome prior to 156.0.8078.79 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-119261	Buffer overflow in Skia in Google Chrome prior to 156.0.8078.79 allowed a remote attacker who had compromised the renderer process to potentially execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2026-103799	Dell PowerProtect Data Domain Management Center, Feature Release versions 7.7.1.0 through 8.8, LTS2024 release versions 7.13.1.0 through 7.13.1.80, LTS2025 release versions 8.3.1.0 through 8.3.1.40, LTS2026 release versions 8.6.1.0 through 8.6.1.20, contain a Missing Authorization vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to unauthorized system operation on managed systems.	9.6	More Details

CVE-2026-62863	MoLing is a computer-use and browser-use based MCP server. Prior to 0.5.0, when MoLing runs in SSE mode using `-l`, its `/sse` and `/message` HTTP endpoints do not authenticate requests and the `mcp-go` dependency sets `Access-Control-Allow-Origin: *`. A malicious web page can open a cross-origin `EventSource` to `/sse`, including a loopback listener, and read the `endpoint` event to obtain `sessionId`. After a victim running SSE mode visits that page, the attacker can use the disclosed `sessionId` against `/message` to send unauthorized MCP tool calls. Depending on the configured tools, those calls can read or write local files, execute commands or perform other actions. Binding only to loopback does not prevent this browser-mediated attack. This issue is fixed in version 0.5.0.	9.6	More Details
CVE-2026-63190	FearlessCMS is a flat-file `content` management system centered on simplicity and open source. Prior to version 0.1.4, five debug/test PHP scripts under `admin/` perform privileged operations without `isLoggedIn()` authentication checks, CSRF protection or adequate `path` validation. On PHP's built-in development server, including the default Docker deployment, `router.php` checks an unnormalized admin URI prefix while the filesystem resolves dot segments, so `/./admin/` bypasses the admin login gate and executes those scripts directly. In `admin/debug_save_flow.php`, attacker-controlled `path` and `content` reach `file_put_contents` for arbitrary `.md` writes under `content`/ or outside it through `path` traversal, enabling site defacement and stored JavaScript in public pages; `print_r($_POST)` output without `htmlspecialchars` escaping also causes reflected cross-site scripting. The `admin/debug_content.php` `path` parameter reaches `scandir()`, `file_get_contents()` and `posix_getpwuid()`, permitting arbitrary directory enumeration and `.md` file reads that expose absolute paths, ownership, permissions, hashes and `content` previews. The `admin/preview-handler.php` endpoint accepts JSON `content` and `title` and writes enumerable files under `content/_preview/`, enabling stored cross-site scripting and disk exhaustion. The `admin/testdebug.php` endpoint appends to `admin/testdebug.log` without authentication, also enabling disk exhaustion. The `admin/test_redirect.php` script exposes a test artifact but escapes its inputs and is not itself an XSS sink. Stored script execution can steal sessions and compromise administrators when they view affected `content`. Reads and writes execute with PHP's privileges; the tested deployment runs PHP as root, amplifying filesystem impact. This issue is fixed in version 0.1.4.	9.4	More Details
CVE-2026-61729	SOCFortress CoPilot focuses on providing a single pane of glass for all your security operations needs. Prior to 0.1.76, `verify_graylog_header` in `backend/app/active_response/routes/graylog.py` and `verify_velociraptor_header` in `backend/app/incidents/routes/incident_alert.py` authenticate webhooks against `GRAYLOG_API_HEADER_VALUE` and `VELOCIRAPTOR_API_HEADER_VALUE` with the same publicly hardcoded fallback. The same default is shipped in `.env.example`. Deployments that leave either setting unset or unchanged permit an anonymous caller with the known header value to bypass the JWT authentication required by normal APIs. `POST /api/graylog/invoke` forwards attacker-selected `COMMAND`, `ACTION`, `VALUE` and `AGENT_ID` to the configured Wazuh manager without the command-enum validation of the authenticated invocation route, allowing active-response scripts to disrupt endpoints and manipulate defensive controls. `POST /api/incidents/alerts/create/threshold` and `POST /api/incidents/alerts/create/velo-sigma` accept forged alerts for arbitrary `customer_code` values and drive attacker-controlled OpenSearch queries. Active-response delivery requires a configured reachable Wazuh manager. Deployments with independently changed header secrets are not subject to this default-secret bypass. This issue is fixed in version 0.1.76.	9.4	More Details
CVE-2026-61730	SOCFortress CoPilot focuses on providing a single pane of glass for all your security operations needs. In affected deployments, the unauthenticated `/scoutsuite-report` `StaticFiles` mount in `backend/copilot.py` exposes the `scoutsuite-report` directory even though normal /api routes require JWT authentication. Generated HTML reports and `scoutsuite-results/scoutsuite_results_<name>.js` files disclose AWS, Azure and GCP IAM principals, resource inventories, misconfigurations and findings. Report names derive from caller-selected names with predictable defaults. During an admin- or analyst-initiated GCP scan, `backend/app/integrations/scoutsuite/routes/scoutsuite.py` saves the uploaded Google service-account JSON key into that same web-served directory. In `backend/app/integrations/scoutsuite/services/scoutsuite.py`, `generate_gcp_report_background` removes the key only after the scan finishes. Any anonymous client that can reach the host and request the file path can therefore retrieve the private key during the scan and use the service account's cloud permissions, as well as read retained cloud-security reports. Credential isolation is released in version 0.1.77; a release fully remediating the report-disclosure component has not been established.	9.3	More Details
CVE-2026-115607	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Crowd Favorite DXP ToolKit dxp-toolkit allows SQL Injection.This issue affects DXP ToolKit: from n/a through 2.0.1.	9.3	More Details
CVE-2026-111411	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Aman FunnelKit Automations wp-marketing-automations allows Blind SQL Injection.This issue affects FunnelKit Automations: from n/a through 3.8.5.2.	9.3	More Details
CVE-2026-39732	Unauthenticated SQL Injection in Transliterator <= 2.5.13 versions.	9.3	More Details
CVE-2026-118762	Monkeytype is a minimalistic and customizable typing test. Prior to 26.43.0, the .github/workflows/fix-formatting.yml workflow runs on pull_request_target with repository write permissions, checks out a fork pull request, installs dependencies from the fork's package.json, and invokes the fork-controlled oxfmt binary. Because actions/checkout persists the elevated GITHUB_TOKEN in Git configuration until after untrusted code executes, an external contributor whose pull request receives the format label can run arbitrary code, read or exfiltrate the token, and push repository content or modify pull requests and issues. The issue affects the repository CI workflow, not the Monkeytype application or user data. This issue is fixed in version 26.43.0.	9.3	More Details
CVE-2026-115964	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in StylemixThemes Motors motors-car-dealership-classified-listings allows Blind SQL Injection.This issue affects Motors: from n/a through 1.4.126.	9.3	More Details
CVE-2026-107034	Insecure permissions in LeafPad / Leaf Note v1.21 (versionCode 21) allows unauthorized attackers to arbitrarily read another user's note data.	9.1	More Details
CVE-2026-55598	PinePods is a complete, self-hosted podcast management system written in Rust. Prior to 0.9.0, an authenticated user can subscribe to an attacker-controlled RSS feed through `POST /api/data/add_podcast` in `rust-api/src/handlers/podcasts.rs`. `get_podcast_values` and `add_episodes` in `rust-api/src/database.rs` parse the feed with `feed-rs` and store the `<enclosure url>` verbatim in `Episodes.episodeurl` without destination host/IP validation. `POST /api/data/download_podcast` invokes `spawn_download_podcast_episode` and `download_episode_and_wait()` in `rust-api/src/services/tasks.rs`, which sends a `reqwest` GET to the stored URL and saves and records the response in `DownloadedEpisodes` for later retrieval. The `estimate_duration_from_audio_url_async()` path in `rust-api/src/database.rs` also sends an unvalidated HEAD during feed add/refresh. Default redirect following permits an initially external enclosure URL to redirect to an internal target. A low-privilege user can make server-side GET/HEAD requests to reachable loopback, private-network and cloud metadata services and read downloaded internal responses, enabling internal-service enumeration, confidential-data disclosure and possible metadata credential theft. Episode downloading requires server downloads to be enabled, which is the default; self-service signup is supported. This issue is fixed in version 0.9.0.	9.1	More Details
CVE-2026-	Insecure permissions in Bulk Share : Location Sender v2.1.0 (versionCode 5) allows unauthorized attackers to invoke an		

107032	exported component, leading to arbitrary data access and control of data flow.	9.1	More Details
CVE-2026-107029	Insecure permissions in rubenalfon Pile v1.1.3 allows unauthorized attackers to invoke an exported component, leading to arbitrary data access and overwriting.	9.1	More Details
CVE-2026-90717	Dell PowerProtect Data Domain Management Center, Feature Release versions 7.7.1.0 through 8.8, LTS2024 release versions 7.13.1.0 through 7.13.1.80, LTS2025 release versions 8.3.1.0 through 8.3.1.40, LTS2026 release versions 8.6.1.0 through 8.6.1.20, contain an Authentication Bypass by Spoofing vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Elevation of privileges. This vulnerability could impact other managed Data Domain systems.	9.1	More Details
CVE-2026-107015	Insecure permissions in Simple Contacts Pro versionCode 107 allow unauthorized attackers to write and read notes in another user's' note database.	9.1	More Details
CVE-2026-107028	Insecure permissions in wbpxre150 Shopping List v11.0 (versionCode 11) allows unauthorized attackers to invoke an exported component, leading to manipulation of the shopping-list data.	9.1	More Details
CVE-2026-116852	Author Remote Code Execution (RCE) in Widget Options <= 4.2.5 versions.	9.1	More Details
CVE-2026-107027	Insecure permissions in lz233 Tarnhelm v1.8.2 (versionCode 20250630) allows unauthorized attackers to invoke an exported component, leading to arbitrary data access and overwriting.	9.1	More Details
CVE-2026-107038	Insecure permissions in Yet Another UPnP Controller versionCode 50200 allows unauthorized attackers to invoke an exported component, leading to arbitrary data access and control of application data.	9.1	More Details
CVE-2026-107021	Insecure permissions in the CardProvider content provider component of helloworld1 AnyMemo versionCode 20260730 allows unauthorized attackers to arbitrarily read flashcards across the user's entire memorization database.	9.1	More Details
CVE-2026-62849	ThingLinks is an enterprise IoT platform. Prior to 1.4.0, an unauthenticated SQL injection vulnerability in the `TDengine TDS APIs` allows request-controlled JSON field values submitted to `/anyUser/tds/insertTableData` to reach unsafe SQL construction in the `TDS mapper`. A remote unauthenticated attacker can tamper with TDengine time-series data, including inserting unintended rows or overwriting existing readings. The affected surface is the TDS module's insert-table-data flow and TDengine mapper SQL generation. This issue is fixed in version 1.4.0.	9.1	More Details
CVE-2026-107017	Insecure permissions in the ShortcutDispatchActivity component of canvoki versionCode 14 allows unauthorized attackers to arbitrarily trigger another user's configured automated actions.	9.1	More Details
CVE-2026-107040	Insecure permissions in MBasov OMN-Go versionCode 26080824 allows unauthorized attackers to invoke an exported component, leading to arbitrary data access and control of data flow.	9.1	More Details
CVE-2026-107056	Insecure permissions in the io.file.importer.ImportActivity component of OpenTracks versionCode 6751 allows unauthorized attackers to inject crafted tracking data into the victim's location database via a crafted SEND message.	9.1	More Details
CVE-2026-107014	Insecure permissions in Bander Notepad (bander.notepad) versionCode 12 allow unauthorized attackers to write and read notes in another user's' note database.	9.1	More Details
CVE-2026-90863	Missing authorization in the administrative interface of Progress Software WS_FTP Server versions prior to 2024.0.7 and 2025.0.4 on Windows could allow a delegated Host Administrator to exceed their authorized scope, potentially enabling arbitrary command execution with elevated privileges and complete compromise of the underlying server.	9.1	More Details
CVE-2026-107053	Insecure permissions in foobnix Librera PDF Reader versionCode 7222 allows unauthorized attackers to arbitrarily write and truncate files in a shared storage space outside of the sandbox.	9.1	More Details
CVE-2026-51863	DB-GPT v0.7.5 and 0.8.0 contains directory traversal in use_example_file (packages/dbgpt-app/src/dbgpt_app/openapi/api_v1/examples_api.py:129). A remote attacker can use the validated exploitation path to write files outside the intended workspace or storage boundary.	9.1	More Details
CVE-2026-117574	A flaw was found in ai-gateway-payload-processing. An authenticated remote attacker can exploit this vulnerability by submitting a request specifying another tenant's model identifier in the request body or header. Because the service does not verify authorization before retrieving credentials from the shared store, it injects the target tenant's application programming interface (API) keys into the request. This flaw allows an attacker to perform unauthorized requests and consume another tenant's large language model (LLM) resources and quotas.	9.1	More Details
CVE-2026-61645	Docat is a tool for hosting versioned static documentation. In the affected implementation, an arbitrary file upload vulnerability in the `Upload API` arises because the API does not validate the `uploaded file path or type`. An attacker can overwrite sensitive configuration files or place malicious files on the Docat web server. Depending on deployment context, uploaded content can enable remote code execution or cross-site scripting intended to steal cookies or redirect users to malicious websites. Version 1.6.0 mitigates filename-based path traversal; remediation of unrestricted file types or deployment-dependent malicious-content effects is not established by the verified patch.	9.1	More Details
CVE-2026-107045	Insecure permissions in the CitrineContentProvider component of Citrine v3.1.0 (versionCode 62) allows unauthorized attackers to arbitrarily read another's Nostr event database.	9.1	More Details
CVE-2026-107043	Insecure permissions in Code Catcher versionCode 131 allow unauthorized attackers to arbitrarily manipulate the app's SMS-code-capture mechanism.	9.1	More Details
CVE-2026-107060	Insecure permissions in Tailscale versionCode 297862600 allows unauthorized attackers to make arbitrary changes to another user's VPN configurations and preferences.	9.1	More Details
CVE-2026-90866	A path traversal vulnerability in Progress Software WS_FTP Server versions prior to 2024.0.7 and 2025.0.4 on Windows could allow a delegated Host Administrator to access locations outside their authorized scope, potentially enabling remote code execution.	9.1	More Details
CVE-2026-67074	HCL BigFix AEX is affected by a Remote Code Execution Vulnerability . It may allow attackers to execute code with the privileges of the affected application or service, potentially leading to unauthorized access, data exposure, or system compromise.	9.1	More Details
CVE-2026-	A path traversal vulnerability in Progress Software WS_FTP Server versions prior to 2024.0.7 and 2025.0.4 on Windows could		

90864	allow a delegated Host Administrator to access or modify files outside their authorized scope.	9.1	More Details
CVE-2026-90865	An OS command injection vulnerability in Progress Software WS_FTP Server versions prior to 2024.0.7 and 2025.0.4 on Windows could allow arbitrary command execution with elevated privileges under certain configurations.	9.0	More Details
CVE-2026-61707	SOCFortress CoPilot focuses on providing a single pane of glass for all your security operations needs. Prior to 0.1.76, in the reported deployment, case-report templates uploaded by `customer_user`, the lowest-privilege portal role, are later executed by non-sandboxed Jinja2 engines when an admin or analyst generates a report. The `/case-report-template/upload` route in `backend/app/incidents/routes/db_operations.py` validates only the filename-derived MIME type, not the template content. Templates share a global store without customer_code scoping, and `customer_user` can also list, download and delete them, allowing an attacker to replace a legitimate default template under the same name. In `backend/app/incidents/services/reports.py`, `render_document_with_context` uses `DocxTemplate` without a sandbox; in `backend/app/incidents/services/reports_pdf.py`, `render_html_template` uses a non-sandboxed `Environment` without autoescaping. Normal privileged requests to `POST /api/incidents/report/generate-report-docx` or `/generate-report-pdf` therefore evaluate attacker-controlled Jinja expressions as Python on the backend. The reported deployment executes commands as root, exposing all tenants' incident and SIEM data and stored connector credentials. The HTML/PDF wkhtmltopdf renderer additionally permits local-file reads and requests to internal services. This issue is fixed in version 0.1.76.	9.0	More Details
CVE-2026-118697	In JetBrains Toolbox App before 3.9.1 and 3.8.2; IntelliJ IDEA, PyCharm, PhpStorm, RubyMine, WebStorm, GoLand and Rider before 2026.3 and 2026.2.4; CLion before 2026.3 and 2026.2.4.1; DataGrip before 2026.3 and 2026.2.6.1; RustRover before 2026.3 and 2026.2.5, the jetbrainsd daemon trusted compromised intermediate certificates	9.0	More Details
CVE-2026-112905	Vvveb is a powerful and easy to use CMS with page builder to build websites, blogs or ecommerce stores. Prior to version 1.0.8.7, authenticated IDOR on admin/auth-token endpoint allows any administrator to read and overwrite another administrator's API tokens. This issue has been patched in version 1.0.8.7.	9.0	More Details
CVE-2026-103693	The Frontend Dashboard WordPress plugin before 3.0.5, ProfileGrid WordPress plugin before 6.0.0.5 do not prevent an unauthenticated user from storing a serialized PHP object in user metadata that is deserialized when a public profile is viewed, allowing PHP object injection that can lead to arbitrary file write and potential remote code execution.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Refe
CVE-2026-45144	Chamilo LMS is an open-source learning management system. From 2.0.0 until 2.0.1, `GET /user/{username}` is anonymously reachable and renders six user-editable profile fields (`firstname`, `lastname`, `competences`, `openarea`, `teach`, and `diplomas`) inside `{% autoescape false %}`, without server-side sanitization on the write path. A ROLE_STUDENT attacker can plant HTML in their own profile; self-registration, when enabled, lets an otherwise anonymous attacker obtain that role. The stored content executes in the browser of any visitor, including administrators, who follows the public profile link, potentially allowing account takeover through session, JWT, or `localStorage` exfiltration. This issue is fixed in version 2.0.1.	8.9	More Deta
CVE-2026-61719	WeGIA is a web manager for charitable institutions. Prior to 3.8.7, a stored cross-site scripting vulnerability in `saude/historico_prontuarios.php` arises because the `textoProntuario` field accepts arbitrary HTML or JavaScript without proper sanitization. An attacker able to create or access a patient's medical record can submit the field through `POST /controle/control.php` with `nomeClasse=SaudeControle`, `metodo=alterarProntuario`, and `id_fichamedica`. The stored content is rendered when another user accesses `/html/saude/historico_prontuarios.php` with `id_historico`, automatically executing attacker-controlled JavaScript in the victim's browser. The vulnerability permits session cookie theft and potential account compromise depending on the victim's privileges. This issue is fixed in version 3.8.7.	8.9	More Deta
CVE-2026-76026	Origin validation error in Autofill in Google Chrome prior to 156.0.8078.79 allowed a remote attacker to bypass web origin policy via a crafted HTML page. (Chromium security severity: High)	8.8	More Deta
CVE-2026-118510	A type-handling flaw in the relationship query building of this MongoDB integration library can cause a check for the absence of a related record to be compiled with an identifier of the wrong data type. In an application that relies on such a check to decide which documents a request may see or act on, a user with basic privileges may be served, may change, or may remove documents that the check was intended to withhold. The failure is silent and produces no error.	8.8	More Deta
CVE-2026-111120	The VikRentCar Car Rental Management System plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.4.8. This is due to missing or incorrect nonce validation on the condtext_update_tmpl function. This makes it possible for unauthenticated attackers to write arbitrary PHP code to the plugin's executable template files such as site/helpers/email_tmpl.php, which are later include()d by loadEmailTemplate() and loadPdfTemplate(), achieving remote code execution on the server via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. The injected PHP payload bypasses sanitization because the plugin's own __PHP_OPEN__/__PHP_CLOSE__ placeholder expansion and cleanPHPSourceCode() logic explicitly reverse both sanitize_text_field filtering and saveHTML() HTML-encoding, restoring a literal <?php...?> payload to live PHP before it is written to disk. Successful exploitation additionally requires an action by an administrator — the attacker cannot trigger the vulnerability on their own.	8.8	More Deta
CVE-2026-104368	The Export and Import Users and Customers plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 2.7.5 via the plugin's own export and re-import workflow. The vulnerability exists because of a CSV escape-character mismatch between the exporter and the importer: class-csvwriter.php writes cells with fputcsv() using PHP's default backslash (\) escape character, while class-csvreader.php parses the same file with fgetcsv() using a double-quote (") as the escape character. As a result, a crafted value stored in a Subscriber's Biographical Info field — containing a backslash-quote sequence followed by a newline — is written as a single quoted CSV field but parsed back as two separate rows on import. The injected second row is then processed by hf_create_customer() as a new user record whose user_login, user_pass, user_email, and role are entirely attacker-controlled, allowing the creation of an arbitrary Administrator account. This makes it possible for authenticated attackers with Subscriber-level access and above to escalate their privileges to Administrator.	8.8	More Deta
CVE-2026-76031	Incorrect authorization in Input in Google Chrome prior to 156.0.8078.79 allowed a remote attacker leveraging social engineering to bypass web origin policy via a crafted HTML page. (Chromium security severity: High)	8.8	More Deta
CVE-2026-76030	Incorrect authorization in FileSystem in Google Chrome prior to 156.0.8078.79 allowed a remote attacker leveraging social engineering to potentially execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Deta

CVE-2026-76029	Improper input validation in Network in Google Chrome prior to 156.0.8078.79 allowed a remote attacker to execute arbitrary code inside the sandbox via crafted network traffic. (Chromium security severity: High)	8.8	More Deta
CVE-2026-76028	Incorrect authorization in FileSystem in Google Chrome prior to 156.0.8078.79 allowed a remote attacker leveraging social engineering to execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Deta
CVE-2026-76025	Incorrect authorization in FileSystem in Google Chrome prior to 156.0.8078.79 allowed a remote attacker leveraging social engineering to execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Deta
CVE-2026-117624	Jenkins 2.587 and earlier, LTS 2.580.1 and earlier does not consistently enforce the restriction on deserializing objects of types marked as storing their configuration in independent top-level configuration files as nested values, allowing attackers to bypass the root element check and potentially inject nested objects.	8.8	More Deta
CVE-2026-119271	Uninitialized resource in Skia in Google Chrome prior to 156.0.8078.79 allowed a remote attacker who had compromised the renderer process to read memory outside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Deta
CVE-2026-119270	Incorrect reference resolution in CacheStorage in Google Chrome prior to 156.0.8078.79 allowed a remote attacker who had compromised the renderer process to obtain sensitive information via a crafted HTML page. (Chromium security severity: High)	8.8	More Deta
CVE-2026-119269	Incorrect authorization in Blink in Google Chrome prior to 156.0.8078.79 allowed a remote attacker to bypass web origin policy via a crafted HTML page. (Chromium security severity: High)	8.8	More Deta
CVE-2026-119268	Use after free in Editing in Google Chrome prior to 156.0.8078.79 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Deta
CVE-2026-119267	Use after free in DOM in Google Chrome prior to 156.0.8078.79 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Deta
CVE-2026-119266	Incorrect reference resolution in Quota in Google Chrome prior to 156.0.8078.79 allowed a remote attacker who had compromised the renderer process to potentially execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Deta
CVE-2026-119265	Incorrect reference resolution in Quota in Google Chrome prior to 156.0.8078.79 allowed a remote attacker who had compromised the renderer process to execute arbitrary code outside the sandbox via crafted network traffic. (Chromium security severity: High)	8.8	More Deta
CVE-2026-117571	The WP Visitor Statistics (Real Time Traffic) WordPress plugin before 8.8 does not sanitize and escape tracking data derived from public visitor requests before storing it and outputting it in the administrative statistics dashboard, allowing unauthenticated attackers to inject arbitrary web scripts that execute when a logged-in administrator views the statistics pages.	8.8	More Deta
CVE-2026-89435	The Formidable Forms – WordPress Form Builder for Contact Forms, Calculators, Quizzes & More plugin for WordPress is vulnerable to Arbitrary Plugin Installation in all versions up to, and including, 6.35 via the 'file_url' parameter parameter. This is due to insufficient URL prefix validation in validate_url_is_in_s3_bucket() and a permission callback that relies solely on a shared token obtainable by any user with the delegable frm_view_forms capability, without checking install_plugins or activate_plugins capabilities. This makes it possible for authenticated attackers, with subscriber-level access and above, to install arbitrary plugins on the server. Exploitation additionally requires that the site is free-only (Formidable Pro is NOT installed).	8.8	More Deta
CVE-2026-119262	Out of bounds write in V8 in Google Chrome prior to 156.0.8078.79 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Deta
CVE-2026-59387	The Nginx routing configuration for Cloud Controller blocks unauthenticated access to /internal/v4/ and /internal/v5/ endpoints but omits an equivalent deny rule for /internal/v3/. As a result, the staging callback endpoints /internal/v3/staging/:guid/droplet_completed and /internal/v3/staging/:guid/build_completed are reachable from the public API listener without OAuth or mutual TLS. An attacker with a valid build or droplet GUID can submit a forged staging callback, transition a droplet to STAGED, and persist arbitrary process metadata and sidecar data with no associated package or actor. A SpaceAuditor can enumerate GUIDs without write permissions, making this an effective privilege escalation beyond the intended role boundary.	8.8	More Deta
CVE-2026-119662	Songloft 2.9.0 before 2.13.6 contains a hardcoded credentials vulnerability that allows adjacent network attackers to authenticate as administrator using the fixed admin/admin pair. Attackers on the same network can log in via the /api/v1/auth/login endpoint to modify library and configuration settings and install JavaScript plugins running in QuickJS.	8.8	More Deta
CVE-2026-103402	An Insufficient Verification of Data Authenticity vulnerability in PCLI in Juniper Networks Session Smart Router and Session Smart Conductor allows an attacker with write access to the model cache directory to execute arbitrary code and escalate privileges via the processing of unverified cache files.	8.8	More Deta
CVE-2026-103403	An Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in AccessManager in Juniper Networks Session Smart Router and Session Smart Conductor allows an attacker to perform arbitrary file deletion and arbitrary command execution via the deletion of an audit rule.	8.8	More Deta
CVE-2026-119654	DataCap through 2025.1.1 contains a missing authorization vulnerability that allows any authenticated user to escalate privileges by calling administrative role and menu management APIs. Attackers, including self-registered accounts, can send PUT requests to /api/v1/user/allocationRole to assign themselves the administrator role and gain full control of the instance.	8.8	More Deta
CVE-2026-103407	An Improper Limitation of a Pathname to a Restricted Directory vulnerability in ConfigDirector in Juniper Networks Session Smart Router and Session Smart Conductor allows an authenticated REST user to read, overwrite, or delete arbitrary certificate and key files on the host filesystem via the certificate and private-key REST API.	8.8	More Deta
CVE-2026-	Dell OpenManage Enterprise, versions prior to 4.8.0, contains an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Command	8.8	More Deta

91913	execution.		
CVE-2026-103408	A Stack Buffer Overflow vulnerability in the DHCP client in Juniper Networks Session Smart Router allows an unauthenticated attacker on the local network to achieve remote code execution via a malicious DHCP reply.	8.8	More Deta
CVE-2026-106079	An Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in AccessManager in Juniper Networks Session Smart Router and Session Smart Conductor allows an attacker with config-write privileges to achieve arbitrary command execution as root in the YANG configuration.	8.8	More Deta
CVE-2026-117612	Jenkins 2.587 and earlier, LTS 2.580.1 and earlier does not apply its deserialization filter to classes referenced by the `resolves-to` attribute during XStream deserialization.	8.8	More Deta
CVE-2026-117614	Jenkins 2.587 and earlier, LTS 2.580.1 and earlier converts the launch commands in older agent configurations into launchers provided by the Command Agent Launcher Plugin without checking whether they have been approved by an administrator, allowing attackers with Agent/Configure permission to execute arbitrary code in the context of the Jenkins controller JVM.	8.8	More Deta
CVE-2026-117616	Jenkins 2.587 and earlier, LTS 2.580.1 and earlier provides an HTTP endpoint that loads agents by name without validating the name, allowing attackers with Overall/Read permission to load any config.xml file on the controller file system as an agent configuration, and to overwrite an arbitrary config.xml file when that agent is saved, potentially resulting in arbitrary code execution.	8.8	More Deta
CVE-2026-119420	Lago through 1.55.0 contains an authentication bypass vulnerability that allows organization administrators to obtain session tokens for existing accounts via the acceptInvite mutation without a password check. Attackers can invite a victim's email, accept with an arbitrary password, and receive a JWT to access the victim's organizations, billing data, API keys and payment integrations.	8.8	More Deta
CVE-2026-109384	The The Innovative Form Builder – IvyForms plugin for WordPress is vulnerable to Arbitrary File Upload in all versions up to, and including, 1.5.1 via the filterFiletypeAndExt function. This is due to insufficient file type validation due to the absence of a dangerous-extension denylist in the allowed-extensions sanitizer and deliberate override of WordPress's native MIME and extension defences via a registered wp_check_filetype_and_ext filter. This makes it possible for authenticated attackers, with custom-level access and above, to upload files that may be executable, which makes remote code execution possible. An authenticated attacker with the custom add_edit_forms capability must first configure a File Upload field with a dangerous extension (e.g., php) in the allowed-extensions list; once that form is published, any unauthenticated visitor can trigger the actual file upload via the publicly accessible /wp-json/ivyforms/v1/form/submission/ REST route.	8.8	More Deta
CVE-2026-119408	n8n before 2.42.6, 2.43.x before 2.43.3, and 3.x before 3.0.1 contains a remote code execution vulnerability via deprecated Function, Function Item, and LangChain Code nodes running outside task runner isolation. Authenticated users who can create, modify, or import workflows naming these hidden node types can execute JavaScript in the n8n main process.	8.8	More Deta
CVE-2026-111505	Dell OpenManage Enterprise, versions prior to 4.8.0, contains an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Command execution.	8.8	More Deta
CVE-2026-110244	IBM Langflow OSS 1.0.0 through 1.12.4 could allow a remote authenticated attacker to obtain sensitive information due to improper limitation of a pathname to a restricted directory.	8.8	More Deta
CVE-2026-65874	This issue affects Apache Fineract versions up to and including 1.15.0. The Center read endpoint (GET /api/v1/centers) and the datatable entry read endpoints (GET /api/v1/datatables/{datatable}/{apptableId} and GET /api/v1/datatables/{datatable}/{apptableId}/{datatableId}) concatenate caller-supplied ordering parameters (orderBy, sortOrder, order) directly into the SQL ORDER BY clause. The existing regex-based input validation can be bypassed, allowing time-based blind SQL injection by any authenticated user with read access to centers or to the targeted datatable. Users are recommended to upgrade to 1.16.1 which fixes the issue.	8.8	More Deta
CVE-2026-119264	Use after free in Dawn in Google Chrome prior to 156.0.8078.79 allowed a remote attacker to potentially execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Deta
CVE-2026-96203	Use after free in Microsoft Edge (Chromium-based) allows an unauthorized attacker to elevate privileges over a network.	8.8	More Deta
CVE-2026-103401	An Improper Link Resolution Before File Access ('Link Following') vulnerability in the unauthenticated web server handlers in Juniper Networks Session Smart Router and Session Smart Conductor allows a local unprivileged user to overwrite arbitrary files as root via unauthenticated API endpoints. This vulnerability can be exploited on Mist-managed routers and on unmanaged Routers that have not yet been onboarded to a Conductor. Routers already managed by Conductor are not affected.	8.8	More Deta
CVE-2026-118081	Contributor PHP Object Injection in 10Web Social Photo Feed <= 1.5.6 versions.	8.8	More Deta
CVE-2026-85890	Double free in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	8.8	More Deta
CVE-2026-104324	IBM Langflow OSS 1.0.0 through 1.12.3 could allow a remote authenticated attacker to execute arbitrary code due to deserialization of untrusted data.	8.8	More Deta
CVE-2026-119144	Frappe Framework before 15.111.0 and 16.x before 16.21.0 contains a server-side template injection vulnerability because user-controlled message fields are rendered as templates without neutralization. An authenticated attacker holding a common operational role can inject template expressions that the server evaluates in an unrestricted context.	8.8	More Deta
CVE-2026-104328	IBM Langflow OSS 1.0.0 through 1.12.3 could allow a remote authenticated attacker to execute arbitrary code due to improper neutralization of special elements used in an OS command.	8.8	More Deta
CVE-2026-107326	IBM Langflow OSS 1.0.0 through 1.12.4 could allow a remote authenticated attacker to execute arbitrary code due to improper neutralization of special elements used in an OS command.	8.8	More Deta

CVE-2026-110193	IBM Langflow OSS 1.0.0 through 1.12.8 could allow a remote attacker with a low-privileged authenticated account to cause the Agentic Assistant to generate or submit component code using these unblocked patterns, resulting in arbitrary operating system command execution on the server.	8.8	More Deta
CVE-2026-118082	Subscriber Privilege Escalation in Buddyboss Platform <= 3.5.0 versions.	8.8	More Deta
CVE-2026-118080	Contributor PHP Object Injection in Social Snap <= 1.5.4 versions.	8.8	More Deta
CVE-2026-88077	Integer overflow or wraparound in Microsoft Edge (Chromium-based) allows an unauthorized attacker to elevate privileges over a network.	8.8	More Deta
CVE-2026-118076	Contributor PHP Object Injection in Frisbii Pay <= 1.8.19 versions.	8.8	More Deta
CVE-2026-118075	Contributor PHP Object Injection in WP Media folders <= 1.1.10 versions.	8.8	More Deta
CVE-2026-118073	Subscriber PHP Object Injection in News Kit Elementor Addons <= 1.5.0 versions.	8.8	More Deta
CVE-2026-116868	Subscriber PHP Object Injection in BuddyPress Xprofile Custom Field Types <= 1.3.1 versions.	8.8	More Deta
CVE-2026-116867	Contributor PHP Object Injection in Dynamic QR Code – generator <= 1.0.1 versions.	8.8	More Deta
CVE-2026-116866	Contributor PHP Object Injection in Extra Fees Plugin for WooCommerce <= 4.4.0 versions.	8.8	More Deta
CVE-2026-110196	IBM Langflow OSS 1.0.0 through 1.12.4 could allow a remote attacker with a low-privileged authenticated account to bypass the administrator-only restriction and execute arbitrary code on the server by configuring a built-in code-execution component with attacker-supplied inputs.	8.8	More Deta
CVE-2026-85897	Heap-based buffer overflow in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	8.8	More Deta
CVE-2026-96192	Use after free in Microsoft Edge for iOS allows an unauthorized attacker to execute code over a network.	8.8	More Deta
CVE-2026-92797	The MemberPress plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.14.1. This is due to a bypassable nonce verification check in the save_profile_fields() function that uses an isset() condition at line 1119, allowing the security check to be completely bypassed by simply omitting the nonce parameter from the request. This makes it possible for unauthenticated attackers to change authenticated users' email addresses via a forged request granted they can trick an authenticated user into performing an action such as clicking on a link, leading to account takeover through password reset functionality.	8.8	More Deta
CVE-2026-51905	TransformerOptimus SuperAGI v0.0.14 is vulnerable to Incorrect Access Control in get_agent_execution_configuration in superagi/controllers/agent_execution_config.py. A remote authenticated attacker from one organization can read another organization's agent execution configuration by supplying the victim agent_id and agent_execution_id to /agent_executions_configs/details/agent_id/{agent_id}/agent_execution_id/{agent_execution_id}. The endpoint lacks an organization ownership check on the selected agent and execution.	8.8	More Deta
CVE-2026-86396	Dell PowerProtect Data Domain, Feature Release versions 7.7.1.0 through 8.8, LTS2024 release versions 7.13.1.0 through 7.13.1.80, LTS2025 release versions 8.3.1.0 through 8.3.1.40, LTS2026 release versions 8.6.1.0 through 8.6.1.20, contain an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to command execution.	8.8	More Deta
CVE-2026-86398	Dell PowerProtect Data Domain, Feature Release versions 7.7.1.0 through 8.8, LTS2024 release versions 7.13.1.0 through 7.13.1.80, LTS2025 release versions 8.3.1.0 through 8.3.1.40, LTS2026 release versions 8.6.1.0 through 8.6.1.20, contain an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to filesystem access for attacker.	8.8	More Deta
CVE-2026-118683	MONAI from 1.2.0 before 1.6.1 contains a remote code execution vulnerability in ConfigWorkflow.__init__, which passes a bundle's configs/logging.conf to logging.config.fileConfig that eval()s handler class and args fields. Attackers can publish a malicious bundle whose logging.conf runs arbitrary Python at workflow construction when a victim loads or runs the bundle.	8.8	More Deta
CVE-2026-86385	Dell PowerProtect Data Domain, Feature Release versions 7.7.1.0 through 8.8, contain an Improper Check for Dropped Privileges vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to elevation of privileges.	8.8	More Deta
CVE-2026-78674	The BPMN System REST APIs do not sufficiently validate input parameters, allowing authenticated users to submit crafted requests that can lead to the execution of arbitrary commands on the server. An authenticated user can leverage this vulnerability to execute arbitrary commands with the privileges of the product's runtime account. The scope of potential damage is contingent upon the permissions assigned to this account.	8.8	More Deta
CVE-2026-	HashiCorp Nomad and Nomad Enterprise are vulnerable to symlink following during same-client allocation data migration that may allow a malicious workload to change permissions and ownership of host directories. This could allow unauthorized access to host data or modification of	8.8	More

119168	host files, potentially leading to privilege escalation. This vulnerability (CVE-2026-119168) is fixed in Nomad 2.1.1 and Nomad Enterprise 2.1.0, 1.11.12, and 1.10.18.		Deta
CVE-2026-86794	The Community Events WordPress plugin before 1.6.0 does not have authorisation or nonce checks when processing public event submissions, and does not escape several of the submitted values before outputting them in the administration dashboard and on the public calendar, allowing unauthenticated users to inject arbitrary web scripts that will execute in the browser of an administrator reviewing the submission.	8.8	More Deta
CVE-2026-115967	Weak Authentication vulnerability in Hamid Alinia Login with phone number login-with-phone-number allows Authentication Abuse.This issue affects Login with phone number: from n/a through 1.8.78.	8.8	More Deta
CVE-2026-96196	Incomplete list of disallowed inputs in Microsoft Edge (Chromium-based) allows an unauthorized attacker to bypass a security feature over a network.	8.8	More Deta
CVE-2026-119028	oapi-codegen 2.0.0 before 2.8.1 contains a code injection vulnerability that allows attackers to inject Go code by supplying non-literal enum entries in integer, number, or boolean schemas. Attackers controlling an OpenAPI document can craft an enum entry that closes the const block in constants.tmpl and injects a func init(), executing code when the generated package is built and imported.	8.8	More Deta
CVE-2026-49142	OpenEMR before 8.5.0 contains an authenticated SQL injection vulnerability in the Syndromic Surveillance module that allows users with Clinician-level privileges to read and modify arbitrary database contents by submitting crafted values in the form_icd_codes[] POST parameter to the syndromicsurveillance/index endpoint. Attackers can inject an unquoted numeric IN() clause and UNION DISTINCT SELECT statement using hex-encoded literals to abuse MySQL extractvalue() for error-based exfiltration of bcrypt password hashes and execute stacked queries that reset passwords, resulting in full administrative account takeover.	8.8	More Deta
CVE-2026-116399	Cross-Site Request Forgery (CSRF) vulnerability in InstaWP InstaWP Connect instawp-connect allows Cross Site Request Forgery.This issue affects InstaWP Connect: from n/a through 0.1.4.2.	8.8	More Deta
CVE-2026-107019	Insecure permissions in the feiertage.ImportActivity component of Arbeitszeiterfassung2 versionCode 159 allows unauthorized attackers to create forged holiday/work-time entries via crafted ICS imports.	8.8	More Deta
CVE-2026-101288	IBM Langflow OSS 1.0.0 through 1.12.3 could allow a remote authenticated attacker to execute arbitrary code due to improper neutralization of special elements used in code.	8.8	More Deta
CVE-2026-96199	Heap-based buffer overflow in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	8.8	More Deta
CVE-2026-96198	Heap-based buffer overflow in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	8.8	More Deta
CVE-2026-119260	Use after free in Frames in Google Chrome prior to 156.0.8078.79 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Deta
CVE-2026-117620	Jenkins 2.587 and earlier, LTS 2.580.1 and earlier allows attackers with Overall/Read permission to trigger warnings in the "Manage Old Data" feature that can be acted on by administrators to inject attacker-controlled data, overriding existing user account information, including login passwords.	8.8	More Deta
CVE-2026-110309	IBM Langflow OSS 1.0.0 through 1.12.4 could allow a remote authenticated attacker to execute arbitrary commands due to improper control of code generation.	8.8	More Deta
CVE-2026-99170	In the Linux kernel, the following vulnerability has been resolved: namespace: a mount that copy_tree() leaves out can't take over a lock Since commit c62a4766937e ("move_mount: transfer MNT_LOCKED") a mount can be moved beneath a locked mount. The lock moves from the old cover to the new mount which takes over the job of hiding what's under it and the old cover can be unmounted. That works as long as the new mount stays. But the caller picks the new mount and copy_tree() leaves a mount of a mount namespace file out of every copy made without CL_COPY_MNT_NS_FILE, together with everything mounted on it, and never looks at MNT_LOCKED. unshare(CLONE_NEWNS) and mount propagation make such copies. So a task that is root in its own user namespace gets rid of a locked cover on a file without a race and without touching the filesystem below it. It makes a child with a mount namespace of its own, binds the child's /proc/<pid>/ns/mnt beneath the cover with MOVE_MOUNT_BENEATH, which hands the lock to that bind, and calls unshare(CLONE_NEWNS). The new mount namespace has nothing on the file. That's the usual way to mask a single file, a bind of /dev/null or of an empty file. With a bind of an ordinary file the file stays covered. copy_tree() already refuses to leave out a locked unbindable mount with -EPERM since commit df7342b24018 ("mount: Don't allow copying MNT_UNBINDABLE|MNT_LOCKED mounts"). Do the same for a locked mount of a mount namespace file. That also covers a tree copied with CL_COPY_MNT_NS_FILE and attached into a mount namespace of another user namespace where lock_mnt_tree() locks it. Note that unshare(CLONE_NEWNS) and clone(CLONE_NEWNS) fail with EPERM from such a mount namespace from then on. The mount can't be left out and it can't be unmounted. And refuse to move a mount of a mount namespace file beneath a locked mount in the first place. Otherwise the task ends up with a mount it can't unmount and an unshare() that fails for good. Chris also found a second mount that goes away by itself, a clone of an automounted mount that shrink_submounts() took along with its parent. Commit f78ddcc87224 ("namespace: never expire a locked mount") took care of that one. Chris's reproducer is appended. Mode nsfile reads SECRET after the unshare() on 7.3-rc7, with this patch the move_mount() fails with EINVAL and the file stays covered. nsfile-control uses an ordinary file and reads MASK both ways. // SPDX-License-Identifier: GPL-2.0 /* * Get rid of a locked cover with MOVE_MOUNT_BENEATH. * * The "admin" (root) makes a tmpfs W: * W/D file, holds SECRET, covered by a bind of a file with MASK * W/Dd/inner file, holds SECRET, Dd is covered by a bind of a directory * whose "inner" holds MASK * W/own directory of uid 1000 with the file "mine" and the * directory "minedir", whose "inner" holds MINE * W/dbg debugfs, mode 755. dbg/tracing is an automount point * The "attacker" is uid 1000. It enters a new user namespace with a new mount * namespace, so W and both covers are locked there. * * usage: prog MODE * plain put a bind of own/mine beneath the cover of D, unmount the cover * nsfile put a bind of the mount namespace file of a child beneath the * cover of D, then unshare(CLONE_NEWNS) * nsfile-control the same with a bind of own/mine * shrink put a bind of the automounted tracefs beneath the cover of Dd, * unmount the cover, put a tmpfs beneath W, call umount(W), which fails * shrink-control the same with a bind of own/minedir * The environment variable AUTOMOUNT_DIR names another automount point for "shrink". */ #define _GNU_SOURCE #include <errno.h> #include <fcntl.h> #include <grp.h> #include <sched.h> #include <signal.h> #include <stdio.h> #include <stdlib.h> #include <string.h> #include <unistd.h> ---truncated---	8.8	More Deta
CVE-	Dell PowerProtect Data Domain, Feature Release versions 7.7.1.0 through 8.8, LTS2024 release versions 7.13.1.0 through 7.13.1.80, LTS2025		More

2026-86378	release versions 8.3.1.0 through 8.3.1.40, LTS2026 release versions 8.6.1.0 through 8.6.1.20, contain a Stack-based Buffer Overflow vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access.	8.8	Deta
CVE-2026-119979	LM Studio before 0.4.22+1 contains a path traversal vulnerability in the model downloader's resolveDownloadRequest that allows attackers to write files outside the models directory using backslash-separated traversal filenames. Attackers can trick users into downloading a crafted model repository that plants a plugin manifest.json, install-state.json and mcp-bridge-config.json, running an attacker-supplied Python payload on every launch.	8.8	More Deta
CVE-2026-118090	Subscriber PHP Object Injection in MasterStudy LMS <= 3.7.55 versions.	8.8	More Deta
CVE-2026-119777	A flaw was found in GStreamer's gst-plugins-bad H.266/VVC parser. When processing a malformed H.266 media file or stream, an integer overflow while parsing profile, tier, and level fields can lead to a stack-based buffer overflow. An attacker could cause an application to crash and may be able to execute code in the context of the affected application.	8.8	More Deta
CVE-2026-116391	Deserialization of Untrusted Data vulnerability in GS Plugins GS Logo Slider gs-logo-slider allows Object Injection.This issue affects GS Logo Slider: from n/a through 3.8.9.	8.8	More Deta
CVE-2026-99185	In the Linux kernel, the following vulnerability has been resolved: firewire: core: fix race condition in split transaction handling For a split transaction, either fw_core_handle_response() or split_transaction_timeout_callback() may manipulate the same transaction entry in the pending transaction list. The return value of timer_delete() is used to determine which function handles the entry. If the transaction is a split transaction and timer_delete() returns zero, the timeout callback may already be running. In this case, the response handler must leave the entry in the list for the timeout callback to remove. A previous code refactoring broke this behavior, introducing a race condition in which both functions could process the same transaction. This could lead to a use-after-free on the transaction initiator side. Fix the regression by ensuring that the response handler does not process the transaction when timer_delete() returns zero. The timeout callback is responsible for removing the entry from the pending transaction list.	8.8	More Deta
CVE-2026-116389	Deserialization of Untrusted Data vulnerability in crossi72 Phoenix Media Rename phoenix-media-rename allows Object Injection.This issue affects Phoenix Media Rename: from n/a through 3.13.5.	8.8	More Deta
CVE-2026-105894	The Ak Framework plugin for WordPress, included in the Newsy - Viral News & Magazine WordPress Theme, is vulnerable to Privilege Escalation in all versions up to, and including, 2.9.8. This is due to missing capability checks in the ajax_refresh_nonce and ak_admin_ajax handlers before passing attacker-controlled option names and values to update_option(). This makes it possible for unauthenticated attackers to update arbitrary WordPress options including users_can_register and default_role to escalate privileges to administrator by enabling user registration with administrator as the default role.	8.8	More Deta
CVE-2026-65566	Cross-Site Request Forgery (CSRF) vulnerability in Meow Apps AI Engine ai-engine allows Cross Site Request Forgery.This issue affects AI Engine: from n/a through 3.8.8.	8.8	More Deta
CVE-2026-73186	Subscriber PHP Object Injection in Enable Media Replace <= 4.2.2 versions.	8.8	More Deta
CVE-2026-59177	ESPHome Device Builder Dashboard is a dashboard for the ESPHome home management software. Prior to 1.0.10, the `Home Assistant` add-on's trusted `ingress` site binds to `0.0.0.0` while intentionally skipping dashboard authentication because the supervisor is expected to authenticate requests upstream. Host networking, required for mDNS, also binds this no-auth site to the `Home Assistant` host's LAN interface. Any device on that local network can therefore connect directly to the `ingress` port, bypass the supervisor, and obtain the full dashboard without credentials or operator misconfiguration. Dashboard capability includes compile-time Python execution through `external_components:`, shell execution through compile and validation subprocesses, and arbitrary access to configuration and data files, compromising the mounted `Home Assistant` configuration and managed ESPHome devices. The standalone Docker dashboard and the password-gated public port 6052 are not affected. This issue is fixed in version 1.0.10.	8.8	More Deta
CVE-2026-1928	The Rank Math SEO – AI SEO Tools to Dominate SEO Rankings plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.0.276 via deserialization of untrusted input in the updateMeta REST API endpoint. This makes it possible forauthenticated attackers, with Contributor-level access and above, to inject a PHP Object. The additional presence of a POP chain allows attackers to achieve remote code execution by writing a webshell to the uploads directory.	8.8	More Deta
CVE-2026-119713	Paperclip 2026.403.0 before 2026.416.0 contains a remote code execution vulnerability that allows agent API key holders to set cleanupCommand and teardownCommand via PATCH /api/execution-workspaces/:id. When the workspace is archived, cleanupExecutionWorkspaceArtifacts runs these commands through a shell as the Paperclip server process, executing attacker-chosen OS commands on the server host.	8.8	More Deta
CVE-2026-78527	Contributor PHP Object Injection in GS Testimonial Slider <= 3.3.10 versions.	8.8	More Deta
CVE-2015-20129	CrushFTP before 7.3.0 contains a cross-site request forgery vulnerability that allows attackers to perform administrative actions because CSRF protection is disabled by default. Attackers can lure an authenticated administrator to a malicious page that submits POST requests to commands like setUserItem, creating root-access users or changing server configuration.	8.8	More Deta
CVE-2026-119332	Ladybird is a truly independent web browser. Prior to 209579c96473c75bd5eba9701fcadb841a045964, FinalizationRegistry::cleanup() in Libraries/LibJS/Runtime/FinalizationRegistry.cpp removed a dead record from m_records, retained an iterator to the next FinalizationRecord, and then invoked attacker-controlled JavaScript through the cleanup callback. If that callback called unregister() for the next record, remove_by_token() freed the node referenced by the retained iterator, and the next cleanup iteration read its target and held_value fields after free. This reliably crashes instrumented WebContent builds and creates a memory-corruption primitive in production builds. This vulnerability is fixed by commit 209579c96473c75bd5eba9701fcadb841a045964.	8.8	More Deta
CVE-	In Trail of Bits fickling through 0.1.12, the _process_import() method in fickle.py adds an imported name to the likely_safe_imports set whenever the source module is present in sys.stdlib_module_names and the name is absent from the UNSAFE_IMPORTS denylist, without inspecting what the name resolves to or how it behaves. The OvertlyBadEvals analysis pass in analysis.py then unconditionally skips any call whose function name appears in likely_safe_imports, including calls that would otherwise be flagged as overtly dangerous. As a result, any callable reachable through a non-blocked standard library module inherits module-level trust regardless of its own behavior, and check_safety() returns LIKELY_SAFE with zero findings for pickle payloads that reach code execution or file write through such callables. Demonstrated primitives: dataclasses._create_fn, which passes an attacker-controlled function body to exec() and yields arbitrary code execution on Python 3.7 through 3.12 (the internal _create_fn function was removed in Python 3.13); mailcap.findmatch, which internally calls os.system() on a test command taken from an attacker-controlled		More

2026-16760	caps dictionary, yielding arbitrary code execution on Python versions through 3.12 (the mailcap module was removed in Python 3.13); and readline.add_history() followed by readline.write_history_file(), which writes attacker-controlled content to an arbitrary filesystem path (POSIX platforms, where the readline module is available). fickling.load() chains check_safety() into pickle.loads() as an explicit security gate, so a LIKELY_SAFE verdict causes the payload to be deserialized and executed with the privileges of the victim process. The root cause is the inference of callable safety from module origin; it is independent of, and separately fixable from, the dotted __qualname__ resolution weakness tracked as CVE-2026-118938, which this advisory does not address. As of 2026-10-30 the three demonstrated modules were added to UNSAFE_IMPORTS on the vendor master branch (commit d011709) pending release; released versions through 0.1.12 remain affected, and the module-origin trust root cause persists, as demonstrated by the related CVE-2026-118938 remaining exploitable on that same build.	8.8	Deta
CVE-2026-118938	In Trail of Bits fickling through 0.1.12, a pickle STACK_GLOBAL operand carrying a dotted __qualname__ (for example "Values.read_file") is resolved by pickle's find_class through _getattribute to an arbitrary attribute path rather than to a module-level function. Fickling records only the leading component of the name in its import tracking and renders the operation as a plain import (for instance, 'python -m fickling' displays it as 'from optparse import Values.read_file'), so the trailing attribute reference is never analyzed as a call. The OvertlyBadEvals analysis pass does not flag it, and check_safety() returns LIKELY_SAFE with zero findings. This allows an attacker to reach a class method that performs code execution: optparse.Values.read_file executes exec(open(filename).read(), vars), achieving arbitrary code execution when the crafted pickle is loaded through fickling.load(), which chains check_safety() into pickle.loads() as an explicit security gate. optparse is present in all current CPython 3.x releases (deprecated as of Python 3.13, not removed). This weakness is in the resolution and analysis of dotted attribute-path names, and is distinct from and independently fixable from the module-origin trust weakness tracked as CVE-2026-16760: resolving or flagging dotted attribute-path imports closes this vector while leaving the module-level trust behavior unchanged. This bypass was verified to remain present on the vendor master branch at commit d011709 as of 2026-10-30, after the vendor's October blocklist additions and a new heuristic that flags private stdlib attributes; because the public class method Values.read_file is neither blocklisted nor flagged as a private attribute, it is not addressed by those remediations.	8.8	More Deta
CVE-2026-56828	Shopper is a Headless e-commerce Admin Panel. From 2.8.0 until 2.8.1, three Shopper Livewire admin components retain authorization gaps after the earlier team-settings authorization fix. A staff member with only `view_users` and `access_dashboard` can mutate permissions, create an administrator, or delete roles. In `packages/admin/src/Livewire/Components/Settings/Team/Permissions.php`, `togglePermission` and `removePermission` authorize `view_users` rather than the stronger `access_setting` permission; `packages/admin/resources/views/livewire/components/settings/team/permissions.blade.php` exposes permission IDs in `wire:click` handlers. The attacker can grant arbitrary permissions to the bound role, including `access_setting` on the attacker's own role, or delete permission definitions. In `packages/admin/src/Livewire/SlideOvers/CreateTeamMember.php`, `mount()` and `store()` also accept `view_users`, and the client-selected `role_id` can identify the admin role, allowing creation of a pre-verified administrator with an attacker-chosen password. In `packages/admin/src/Livewire/Pages/Settings/Team/RolePermission.php`, `deleteAction` has no action authorization and is only conditioned on `can_be_removed`, while page access requires `view_users`. Deleting a removable role removes access for assigned users, enabling RBAC denial of service as well as privilege escalation. This issue is fixed in version 2.8.1.	8.8	More Deta
CVE-2026-116778	FOG is a free open-source cloning/imaging/rescue suite/inventory management system. Prior to 1.5.10.2253 and 1.6.0-RC-1, an authenticated API-enabled user with uType=1 who possesses both the user's API token and the global FOG API token can use PUT /fog/storagenode/{id}/edit to modify Storage Node user, pass, and ftppath fields because the API validates the credentials but does not enforce an administrator-only role. With storage replication enabled and a usable Storage Node, FOGImageReplicator interpolates those fields into an lftp command executed through proc_open() by the root-running service, allowing the low-privileged user to execute commands as root. This issue is fixed in versions 1.5.10.2253 and 1.6.0-RC-1.	8.8	More Deta
CVE-2014-125138	C97net qEngine CMS through 6.0.0, Kemana Directory through 1.5.6, and Cart Engine through 3.0.0 contain an unrestricted file upload vulnerability in administrative image fields. Editor-role users can upload PHP scripts via the page_image or cat_image parameters to the web-accessible /public/image directory and request them to execute code on the server.	8.8	More Deta
CVE-2026-118086	Subscriber Privilege Escalation in WP BASE Booking <= 6.5.2 versions.	8.8	More Deta
CVE-2026-118645	n8n before 1.123.85, 2.x before 2.43.5, and 2.44.x before 2.44.1 contains a filter injection vulnerability in the Quick Base node, which sends the Where filter to the Quick Base API as raw query text. Attackers supplying untrusted input such as webhook data used to build the filter can make Get Many return every record or Delete remove every record with the workflow credential's privileges.	8.7	More Deta
CVE-2026-62990	Shopper is a Headless e-commerce Admin Panel. In versions from 2.0.0 prior to 2.10.1 and in the 3.0.0 prereleases beta.1 and beta.2, authenticated back-office staff with a content-upload permission can store executable media on the administrator's own origin. In the 2.x implementation, relevant upload permissions include `edit_products` or `add_brands`, and `packages/admin/config/media.php` allows `image/svg+xml` in every media collection, including image fields whose image/* validation also accepts SVG. The product files collection in `packages/admin/src/Livewire/Components/Products/Form/Files.php` has no MIME restriction and accepts `text/html` as well. Media is served inline from the `public` disk under `/storage/` with its own content type, without `Content-Disposition: attachment` or a `Content-Security-Policy`. When an administrator opens an uploaded HTML or SVG file, stored script executes in that administrator's session. In 2.x, the script can invoke `packages/admin/src/Livewire/SlideOvers/CreateTeamMember.php`, whose `store()` checks `access_setting` held by the viewing administrator but trusts client-supplied `role_id`, to create a new attacker-controlled administrator with a chosen password. This account persists after the uploaded file is deleted and gives access to customer data, orders, settings, and user/role management; the same script can exfiltrate data or grant permissions to the attacker's account. Direct account creation by the low-privileged uploader is blocked, so exploitation requires the administrator to open the file. The 3.x prerelease line already excludes SVG but still allows executable product files. This issue is fixed in versions 2.10.1 and 3.0.0-beta.3.	8.7	More Deta
CVE-2025-8574	The Database Cleaner plugin for WordPress is vulnerable to arbitrary table deletion in all versions up to, and including, 1.4.7. This is due to a lack of restriction on database tables that can be deleted. This makes it possible for authenticated attackers, with Administrator-level access and above, to delete core WordPress tables.	8.7	More Deta
CVE-2026-13303	HashiCorp Boundary and Boundary Enterprise are vulnerable to a server-side request forgery in the Vault credential store integration that may allow an authenticated user with permission to manage credential stores and credential libraries within a project to cause the Boundary controller to issue outbound requests to a network destination of the requester's choosing and to receive the response. This may expose endpoints reachable only from the controller's host, such as a cloud instance metadata service. This vulnerability, CVE-2026-13303, is fixed in Boundary Enterprise 1.0.2 and 0.21.6.	8.7	More Deta
CVE-2026-119572	Traefik from 3.7.0-ea.1 before 3.7.15 contains an authentication bypass vulnerability in the Kubernetes Ingress NGINX provider that silently disables mTLS configured via the auth-tls-secret annotation. When another Ingress declares a path on the same host without matching auth-tls settings, Traefik falls back to default TLS options, letting unauthenticated attackers reach backends requiring client certificates.	8.7	More Deta
CVE-2026-113387	The Ortto plugin for WordPress before 1.0.25 did not authenticate configuration update requests, relying only on a secret exposed in public HTML. An unauthenticated threat actor could overwrite the plugin's configuration to serve arbitrary scripts.	8.6	More Deta

CVE-2026-111419	A sensitive information exposure vulnerability exists on the Foxit official website because JavaScript code contains third-party authorization information. This may allow unauthorized parties to obtain or misuse the exposed credentials.	8.6	More Deta
CVE-2026-89216	The vTables WordPress plugin before 0.3 does not properly sanitise and escape a parameter before using it in a SQL statement, which allows unauthenticated attackers to perform SQL injection attacks and extract data from the database.	8.6	More Deta
CVE-2026-67073	HCL BigFix AEX is affected by an Unrestricted File Upload and Improper Access Control vulnerability. This could allow an attacker to upload malicious or unauthorized files and directly access or download sensitive uploaded content, potentially leading to information disclosure, unauthorized access, or system compromise.	8.6	More Deta
CVE-2026-40573	NovumOS is a custom 32-bit operating system written in Zig and x86 Assembly. Prior to version 0.25-beta.1, the `Nova` interpreter runs in Ring 0 with unrestricted kernel-memory access. Loading a malicious `.nv` script through the shell permits a local user to execute code with kernel privileges without security checks. The advisory identifies VM initialization in `zig/nova/vm.zig` as the affected component; script execution is not isolated in a restricted Ring 3 privilege domain. This issue is fixed in version 0.25-beta.1.	8.6	More Deta
CVE-2026-61542	Gearboy is a Game Boy, Game Boy Color, and Super Game Boy emulator and debugger with an embedded MCP server. Gearsystem, the affected component, has an optional `--mcp-http` mode that accepts unauthenticated MCP requests from any reachable network peer despite localhost-only documentation and logging. In the described `platforms/shared/desktop/mcp/mcp_transport.h` transport, the socket binds `INADDR_ANY`, normally on port 7777, and POST requests to `/mcp` reach dispatch without `Authorization`, `Host`, or `Origin` checks. Responses and OPTIONS advertise `Access-Control-Allow-Origin: *`. A peer can initialize an MCP session and invoke exposed emulator/debugging operations; even a garbage bearer token does not block dispatch, while a loopback-bind negative control prevents network access. The reported impact is bounded to the emulator process, debugging state, and local files accepted as media, rather than demonstrated host code execution. Gearboy 3.8.7 contains a patch.	8.6	More Deta
CVE-2026-76418	A vulnerability in the Remote Access SSL VPN service of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to logic errors when secondary authentication is configured on a tunnel group. An attacker could exploit this vulnerability by sending a crafted request when connecting to the SSL remote access VPN. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.	8.6	More Deta
CVE-2026-118660	Happy DOM is a JavaScript implementation of a web browser without its graphical user interface. Prior to 21.0.0, Happy DOM loads iframe src URLs and link rel="stylesheet" href URLs by default while parsing untrusted HTML on the server because disableIframePageLoading and disableCSSFileLoading default to false. An attacker who controls parsed HTML can therefore cause server-side requests to arbitrary internal or cloud endpoints without an application opt-in and may expose confidential responses or credentials returned by those endpoints. This issue is fixed in version 21.0.0.	8.6	More Deta
CVE-2026-61572	AVideo is a video-sharing Platform. Before the initial remediation attempt in 8.1.0, `url_get_contents` in `objects/functions.php` accepts caller-controlled destinations after only `FILTER_VALIDATE_URL` syntax validation, without rejecting private, loopback, or link-local addresses, and disables TLS peer verification. `Login::isLogged` reauthenticates using the attacker-settable `encoder_aVideoURL` cookie together with arbitrary nonempty `encoder_user` and `encoder_pass` cookies, and `Login::run` stores the raw fetched body in `result`. The unauthenticated `objects/login.json.php` endpoint returns that session object, enabling full-response exfiltration through a supplied `siteURL`; its `Streamer::isURLAllowed` gate allows all sites when the operator allowlist is empty, the default. An unauthenticated remote attacker can read internal HTTP and HTTPS responses, including cloud instance-metadata credentials, and reach internal TCP services. A further pre-authentication FTP variant in `view/youtubeDl.json.php` routes an ftp `videoURL` into `FTPDownloader`; `parseFtpUrl` in `objects/FTPDownloader.php` accepts its host and port for `ftp_connect`. This also enables requests to internal FTP services. Untrusted self-signed HTTPS certificates are accepted, and no account or operator interaction is required. Version 8.1.0 contains an initial remediation attempt that removes raw-response reflection and adds destination checks, but private-network exemptions and login TLS-verification defaults leave complete remediation of the described internal-network and TLS variants unresolved.	8.6	More Deta
CVE-2026-103092	IBM Langflow OSS 1.0.0 through 1.12.3 could allow a remote authenticated attacker to execute arbitrary SQL commands due to improper access control.	8.5	More Deta
CVE-2026-39736	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Crocoblock JetEngine jet-engine allows SQL Injection.This issue affects JetEngine: from n/a through 3.9.0.1.	8.5	More Deta
CVE-2026-61996	Subscriber SQL Injection in MLS On The Fly <= 1.8.1.5 versions.	8.5	More Deta
CVE-2026-119115	Incorrect authorization in the issuer resolution logic in AWS Private CA Connector for Kubernetes (aws-privateca-issuer) before v1.10.1 might allow an authenticated remote user to obtain certificates, including subordinate CA certificates, signed by a cluster-scoped AWS Private CA issuer that their approval policy does not authorize. To remediate this issue, users should upgrade aws-privateca-issuer to version v1.10.1 or the AWS Private CA Connector for Kubernetes EKS add-on to version v1.10.1-eksbuild.1, and update any certificate requests, Certificate resources, or Ingress annotations whose issuerRef.kind is missing, incorrect, or does not match the referenced issuer, since v1.10.1 requires issuerRef.kind to be exactly AWSPCAIssuer or AWSPCAClusterIssuer and to match the issuer it references.	8.5	More Deta
CVE-2026-115965	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in BuddyPress BuddyPress buddypress allows Blind SQL Injection.This issue affects BuddyPress: from n/a through 14.5.2.	8.5	More Deta
CVE-2026-116239	In server mode pgAdmin 4 keeps an account per authentication source, so the same username can exist as, for example, an internal account and an LDAP account. After LDAP or Kerberos authenticated a user, pgAdmin chose the account to log in by username alone, or took the account Flask-Security's login form had looked up, without checking that it came from the source that authenticated the user. The session therefore belonged to another account, with its role, its servers and its saved database passwords: - An LDAP or Kerberos user whose username matched an internal account was logged in as that internal account, including the administrator account created when pgAdmin is first set up. - With internal authentication listed before LDAP or Kerberos in AUTHENTICATION_SOURCES, the login form's internal validation looks up the account whose email was typed and keeps it even though its password does not match. A Kerberos user could type another Kerberos user's principal and be logged in as that user, and an LDAP user could do the same with an LDAP account whose email is their username. Exploitation requires valid credentials for an LDAP directory or Kerberos realm that pgAdmin is configured to use. The fix looks the account up by the authenticated username and the source that authenticated it, and no longer uses the account the login form found for any source but internal authentication. Internal authentication logs in that account only if it is an internal account. Desktop mode is not affected. This issue affects pgAdmin 4: before 9.19.	8.5	More Deta
	SOCFortress CoPilot focuses on providing a single pane of glass for all your security operations needs. Prior to 0.1.76, `POST`		

CVE-2026-61708	/api/agent_data_store/upload` in `backend/app/data_store/data_store_routes.py` permits `customer_user` callers to choose `bucket_name` and `object_name` without an allowlist, tenant prefix, ownership check or content restriction. The only file check requires a nonempty filename. The operations in `backend/app/data_store/data_store_operations.py` create missing buckets and upsert objects, allowing existing objects belonging to any tenant to be overwritten. Targets include `sysmon-configs/<customer_code>/sysmon_config.xml` distributed to managed Windows endpoints, `copilot-case-report-templates/<name>` rendered server-side, and case evidence or forensic artifacts under `copilot-cases/<case_id>/<file>` and `velociraptor-artifacts/<agent_id>/<flow_id>/<file>`. A lowest-privilege user can tamper with cross-tenant evidence, blind endpoint telemetry, poison report templates for later code execution, plant data or exhaust storage. Sibling list, download and delete routes remain restricted to admin/analyst; the exposed operation is the upload write path. This issue is fixed in version 0.1.76.	8.5	More Deta
CVE-2026-59185	identrail is a machine identity security platform for AWS, GitHub/OIDC, and Kubernetes. Prior to 1.0.2, the default-on `POST /v1/workspaces/:workspace_id/projects/:project_id/github/connect/complete` endpoint in `internal/api/router.go` accepts `installation_id` from the request body or `X-GitHub-Installation-ID` header without verifying the installation belongs to the caller's workspace. `CompleteGitHubConnection` in `internal/api/github_connect.go` rigorously binds `state` to the caller's tenant, workspace, and project, but checks only that the installation ID is positive before persisting it as the caller's connection. `ListInstallationRepositories` in `internal/connectors/github/repositories.go` invokes token creation through `internal/connectors/github/app.go` and `POST /app/installations/{installationId}/access_tokens`, using the application's JWT. An authenticated tenant who starts a legitimate connection can supply another customer's non-secret installation ID to read the victim organization's private repository inventory, content, and metadata or drive posture scans, provided identrail's GitHub App is installed there. The default-off V2 `CompleteGitHubConnector` path shares the installation-ownership gap and additionally matches pending `state` without rechecking caller scope. This issue is fixed in version 1.0.2.	8.5	More Deta
CVE-2026-111850	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in BuddyPress BuddyPress buddypress allows SQL Injection.This issue affects BuddyPress: from n/a through 14.5.2.	8.5	More Deta
CVE-2026-119978	Flowise through 3.1.4 contains a sandbox escape vulnerability that allows authenticated users to execute OS commands by abusing allowlisted langchain and mammoth modules when ALLOW_BUILTIN_DEP=true. Attackers can submit JavaScript to /api/v1/node-custom-function that writes a file into the mammoth package via LocalFileStore and requires it, escaping vm2 as the Flowise process user.	8.5	More Deta
CVE-2026-115603	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Advanced Ads GmbH Advanced Ads – Tracking advanced-ads-tracking allows Blind SQL Injection.This issue affects Advanced Ads – Tracking: from n/a before 4.0.0.	8.5	More Deta
CVE-2026-116249	In server mode pgAdmin 4 resolves a server's password file, SSL certificate, key, CRL and SSH tunnel identity file relative to the user's storage directory, but get_complete_file_path() only stripped leading slashes before joining the two. A path such as "../<another user>/.pgpass", set through the server dialog, the REST API or a servers.json import, therefore named another user's file, and connecting used that user's saved passwords, client certificate or SSH key. The sslkeylogfile connection parameter was passed to libpq unchanged, so a path outside storage let libpq create or append a file as the account running pgAdmin. make_conninfo() also quoted connection parameter values but not their names, so a crafted parameter name could smuggle additional keyword=value pairs past these checks. The fix requires the resolved path, with symbolic links followed, to stay inside the user's storage directory or the named shared storage directory, confines sslkeylogfile the same way, and accepts only exact libpq keywords as connection parameter names. A refused path or keyword is reported instead of letting libpq fall back to a default. This issue affects pgAdmin 4: before 9.19.	8.4	More Deta
CVE-2026-118992	CallBackery versions before 0.62.0 for Perl allow OS command execution via sqlite3 shell commands in a restored configuration backup. restoreConfigBlob() feeds the database dump in a backup to the sqlite3 command-line shell. The shell runs lines starting with a dot as its own commands, so .shell or .system in the dump runs an OS command and .load loads native code. Anyone who can supply a backup to be restored can run arbitrary commands as the application user.	8.4	More Deta
CVE-2026-107347	HashiCorp Nomad and Nomad Enterprise are vulnerable to symlink following during dispatch payload and executor log writes that may allow a malicious workload to modify files outside its allocation directory. When the client agent runs as root, this could lead to code execution as root on the client host. This vulnerability (CVE-2026-107347) is fixed in Nomad 2.1.1 and Nomad Enterprise 2.1.0, 1.11.12, and 1.10.18.	8.4	More Deta
CVE-2026-99216	In the Linux kernel, the following vulnerability has been resolved: Drivers: hv: Don't reset VMBus connection state on error/exit paths In two places, current code forces vmbus_connection.conn_state to DISCONNECTED prior to calling vmbus_disconnect(). But vmbus_disconnect() calls vmbus_initiate_unload(), which unloads the VMBus connection only if the conn_state is CONNECTED. Consequently, the connection remains and the Hyper-V host might continue to send messages or post VMBus interrupts. The problem was introduced in commit 74347a99e73ae ("x86/Hyper-V: Unload vmbus channel in hv panic callback"), in that vmbus_initiate_unload() started checking the current connection state before doing the unload. This commit removed some occurrences where conn_state was forced to DISCONNECTED, but these two remained, apparently due to an oversight at the time. Fix this by not forcing conn_state to DISCONNECTED during VMBus exit, or if a failure occurs when establishing the connection in the first place. Whatever value conn_state has at the time is then read by vmbus_initiate_unload() to determine if there is a connection to be unloaded.	8.4	More Deta
CVE-2026-45049	Open Access Management (OpenAM) is an access management solution. Prior to 16.1.1, the `Cross-Domain Single Sign-On` (`CDSSO`) servlet allows a logged-in user's raw OpenAM session token to be POSTed to an attacker-controlled URL. An attacker who induces an authenticated victim to visit a crafted URL can receive the session credential and potentially hijack the session. Deployments must have `CDSSO` enabled, as is common in multi-domain deployments, and exploitation is additionally gated on a non-default configuration being absent. This issue is fixed in version 16.1.1.	8.3	More Deta
CVE-2026-103779	Dell PowerProtect Data Domain, Feature Release versions 7.7.1.0 through 8.8, LTS2024 release versions 7.13.1.0 through 7.13.1.80, LTS2025 release versions 8.3.1.0 through 8.3.1.40, LTS2026 release versions 8.6.1.0 through 8.6.1.20, contain an Improper Authentication vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Protection mechanism bypass.	8.3	More Deta
CVE-2026-59179	OpenHop is a tool for creating interactive data-flow diagrams. Prior to 0.3.7, `@openhop/server` passes unauthenticated flow route parameters from `GET /api/flows/:id` and `DELETE /api/flows/:id` in `packages/server/src/routes.ts` to `FlowStore.filePath()` in `packages/server/src/store.ts` without an identifier allow-list. The router applies `decodeURIComponent` to the id, and `path.join()` then normalizes traversal outside the configured flow directory after appending the .yaml extension. An attacker can read accessible YAML files as YAML-parsed JSON or permanently delete accessible .yaml files outside that directory, exposing configuration or secrets and disrupting dependent services. In `packages/server/src/index.ts`, CORS `origin: true` permits any browser origin, enabling a malicious webpage to target a loopback-bound instance. Docker deployments default to `HOST=0.0.0.0` and permit direct unauthenticated network access. This issue is fixed in repository release 0.3.7.	8.3	More Deta
CVE-2026-	YosemiteCrew provides organization-based service and task management. In the source-reported affected main and dev snapshots, YosemiteCrew's service and PMS task-library/template routes omit organization and permission checks. `authorizeCognito` in `apps/backend/src/middlewares/auth.ts` sets the authenticated user's ID but does not provide the `withOrgPermissions()` and `requirePermission(...)` checks used by protected siblings. In `apps/backend/src/routers/service.router.ts`, `PATCH /fhir/v1/service/:id` and `DELETE /fhir/v1/service/:id` are authentication-only, while `GET /fhir/v1/service/:id` has no authentication middleware. The trace through `apps/backend/src/controllers/web/service.controller.ts` to `apps/backend/src/services/service.service.ts` passes a global record ID into `ServiceModel.findById(oid)` without an `organisationId` filter. In `apps/backend/src/routers/task.router.ts`, `PUT /v1/task/pms/library/:libraryId`,	8.3	More

59979	`POST /v1/task/pms/templates`, `PATCH /v1/task/pms/templates/:templateId` and `DELETE /v1/task/pms/templates/:templateId` likewise lack organization/role enforcement. Any registered platform user, including a patient/companion-app account, can modify or delete another organization's service catalogue and PMS task-library/template data, affecting bookings and billing; service records can additionally be read without authentication. An earlier security change protected create routes but left these sibling operations exposed. A fixed release cannot be established from the available evidence.		Deta
CVE-2026-115642	In OpenStack keystonemiddleware before 13.0.2, by supplying a custom X-Service-Token header in a request, anyone in possession of an access-restricted application credential may bypass those restrictions resulting in elevation of privileges.	8.3	More Deta
CVE-2025-14260	Due to the improper implementation of access control rules, malicious actors could perform a Server Side Request Forgery (SSRF) attack on affected WSO2 Products. Exploiting this vulnerability allows a malicious actor to access both internal and external resources, available through the network or filesystem. This could potentially lead to unauthorized access to sensitive data and systems, regardless of whether these resources are located within a private network, as long as they are reachable by the WSO2 product.	8.3	More Deta
CVE-2026-118649	n8n before 2.43.5 and 2.44.x before 2.44.1 accepts a client-supplied workflow ID and caches each workflow's owner project in memory by that ID, so a crafted ID such as __proto__ makes the Data Table project check match every project. An authenticated member who can create and run workflows can list, read, modify, and delete Data Table rows in all projects of the instance.	8.3	More Deta
CVE-2026-116245	libpq looks a connection service up in the service file of the operating-system account running pgAdmin 4, and an entry there can hold a password or name a password file or client certificate. In server mode any user could set a server's Service, or a "service" connection parameter, to one of those entries and connect with its credentials. A PGPASSWORD or PGSERVICE variable set for that account was likewise used by libpq for every connection without a value of its own and passed on to the utilities, and pg_dumpall read a maintenance database name such as "service=..." as a connection string. The fix adds the SERVER_MODE_ALLOWED_SERVICES setting, empty by default: in server mode only a listed service can be used, the servicefile parameter is refused, and PGPASSWORD and PGSERVICE are removed from pgAdmin's environment at startup. The allowlist is checked again on the final connection string, and the pg_dumpall database name is wrapped as a connection string. This issue affects pgAdmin 4: before 9.19.	8.2	More Deta
CVE-2026-9535	A out-of-bounds read vulnerability exists in the vtkChacoReader InputGraph2 functionality of vtk (version(s): 9.6.1). A specially crafted chaco can lead to an out-of-bounds read. An attacker can provide a malicious file to trigger this vulnerability.	8.2	More Deta
CVE-2026-62331	praktor is a multi-agent Claude Code orchestrator with Telegram input and output, Docker isolation, and a Mission Control UI. Prior to 0.9.1, both Telegram upload sites in `internal/telegram/bot.go` concatenate the attacker-controlled document filename into a destination path without sanitization, and `path.Join` collapses parent-directory traversal. A remote Telegram user who can message the bot can therefore write outside `uploads/` within the persistent agent workspace mounted at `/workspace/agent`. Because `allow_from: []` permits all senders by default, no prior authentication or privilege is required in that configuration. The attacker can plant or overwrite `CLAUDE.md`, instruction, skill, hook, or configuration files that the Claude agent reads and operates on across later runs, turning a document upload into stored instruction injection. The demonstrated arbitrary-write scope is the persistent agent workspace volume, not an unrestricted host-filesystem write. This issue is fixed in version 0.9.1.	8.2	More Deta
CVE-2026-116247	When a server in pgAdmin 4 had no password file, client certificate or client key configured, or the configured one could not be found, pgAdmin left the parameter out of the connection and libpq fell back to the defaults of the operating-system account running pgAdmin: ~/.pgpass, ~/.postgresql/postgresql.crt and postgresql.key, or PGPASSFILE, PGSSLCERT and PGSSLKEY. In server mode any user could therefore connect to a server with the service account's saved passwords or client certificate, and supplying only a copy of its public certificate was enough for libpq to pair it with the service account's private key. A pg_service.conf entry, or a maintenance database name read as a connection string by pg_dumpall, could bring the same files back for the utilities. The fix gives each of these parameters a value in server mode, the user's own file or otherwise a path that can never be opened, in the connection string, in the environment of the utilities and in the --dbname connection string that ranks above a service entry. Desktop mode is unchanged. This issue affects pgAdmin 4: before 9.19.	8.2	More Deta
CVE-2026-115709	Improper Link Resolution Before File Access ('Link Following') (CWE-59) in Elastic Cloud Enterprise (ECE) can lead to unauthorized disclosure and loss of data belonging to other deployments on the same host via Symlink Attack (CAPEC-132).	8.2	More Deta
CVE-2026-118643	n8n before 1.123.85, 2.x before 2.43.5, and 2.44.x before 2.44.1 stores credential secrets in execution error data when operations fail in the Git, MongoDB Atlas Vector Store, and Google Cloud Storage nodes. Users who can view a workflow's executions but cannot read the credential can recover Git passwords or tokens, MongoDB database passwords, or Google access tokens from that data.	8.2	More Deta
CVE-2026-118647	n8n before 1.123.85, 2.x before 2.43.5, and 2.44.x before 2.44.1 saves the SeaTable Trigger node's API token in error execution data, because failed poll requests store raw request headers. Users who can view workflow executions but cannot read the credential can recover the token and access the connected SeaTable base.	8.2	More Deta
CVE-2026-58412	Filecoin Pin is an IPFS Pinning Service API implementation that pins to Filecoin's PDP service. Prior to 1.1.0, the upload GitHub Action's fork detection in `upload-action/src/build.js` checks only `event.pull_request`. In the documented two-workflow pattern, an untrusted fork pull-request workflow produces an artifact and a privileged `workflow_run` workflow downloads and uploads it. Because `workflow_run` has no `event.pull_request`, `isForkPR` becomes false and `uploadStatus` becomes `pending-upload`. The action later resolves `workflow_run.pull_requests` without repeating the fork check before initializing the wallet with `walletPrivateKey` and uploading the artifact. An external contributor can therefore cause attacker-controlled artifacts to be stored using the repository owner's Filecoin wallet, incurring unauthorized storage expenditure, dataset pollution and consumption of configured wallet funds. Disclosure of the wallet private key is not required. The 0.x action line is not receiving a backport and must be migrated to a fixed 1.x release. This issue is fixed in version 1.1.0.	8.2	More Deta
CVE-2026-116242	pgAdmin 4 opens SSH tunnels with the sshtunnel library but gave it neither host_pkey_directories nor ssh_config_file, so it always loaded the unencrypted private keys in ~/.ssh of the operating-system account running pgAdmin, read that account's ~/.ssh/config (IdentityFile, User, HostName, ProxyCommand) for the tunnel host, and could use its ssh-agent. In server mode any user could therefore configure a tunnel to a host that accepts the service account's key, with no credentials of their own or with an identity file that did not exist in their storage, and reach it as that account. The fix makes tunnels in server mode use only the identity file or password the user configured: the service account's keys, configuration and agent are no longer used, and an identity file that cannot be found in the user's storage is reported instead of falling back to ~/.ssh. Desktop mode is unchanged. This issue affects pgAdmin 4: before 9.19.	8.2	More Deta
CVE-2026-61854	VoiceSentinel is a real-time voice moderation system for Minecraft servers. From 2.2.1 until 3.3.1, the optional report buffer feature has a race between retention cleanup and normal transcript writes. In `report_buffer.py`, `_maybe_cleanup()` uses an unlocked dictionary for once-per-hour cleanup throttling, allowing simultaneous `_cleanup_tenant()` operations for one tenant. Cleanup reads `transcripts.jsonl` and rewrites it in place without file locking or atomic replacement, while `report_buffer_append_async` uses `asyncio.to_thread` to append without synchronization. In `main.py`, concurrent `_processing_worker` tasks make this reachable in normal operation; `processing.worker_count` of two or more and public-pool servers sharing a `server_key` increase collisions. With `report_buffer.enabled` set to true, racing writes can lose, duplicate or corrupt	8.2	More Deta

	transcript data and defeat `report_buffer.retention_seconds` pruning, allowing unbounded disk growth that can exhaust storage and crash the host or other services sharing it. The feature is opt-in and disabled by default. This issue is fixed in version 3.3.1.		
CVE-2026-62847	Metalama is a Roslyn-based open-source patterns and architecture toolkit for C#. Prior to 2025.1.18, 2026.0.25 and 2026.1.19, Metalama.Framework and Metalama.Tool load and execute compile-time assemblies, auxiliary executable tools and embedded helper assemblies from predictable temporary directories. On `Linux` and `macOS`, the default `Path.GetTempPath()` location is world-writable, and existing artifacts are trusted based on sentinel or `.completed` marker files rather than integrity verification. A local unprivileged user on a shared machine or CI/build agent can pre-create the deterministic directory structure and plant a malicious DLL with the matching sentinel. When a higher-privileged developer or build account subsequently builds, Metalama skips regeneration and executes the planted artifact in the compiler, IDE or MSBuild process as the building user. This permits cross-user privilege escalation, reading source and secrets, supply-chain tampering with build output, or disrupting builds. Default Windows per-user temporary directories are protected by ACLs and are not affected. Deployer-selected insecure cache locations are outside the vulnerability's scope. This issue is fixed in versions 2025.1.18, 2026.0.25 and 2026.1.19.	8.2	More Deta
CVE-2026-99131	In the Linux kernel, the following vulnerability has been resolved: xfs: fix capability check in xfs An user reported a bug where he managed to evade group's quota by changing a file's gid to a different group id the same user belonged to, even though quotas were enforced on both gids and the file's size was big enough to exceed the quota's hardlimit. Commit eba0549bc7d1 replaced a capable() call by a has_capability_noaudit() to prevent unnecessary selinux audit messages. Turns out that both calls have slightly different semantics even though their documentation seems similar. Where in a nutshell: capable() - Tests the task's effective credentials has_ns_capability_noaudit() - Tests the task's real credentials This most of the time has no practical difference but in some cases like changing attrs (specifically group id in this case) through a NFS client this will allow the quota code to use XFS_QMOPT_FORCE_RES, effectively bypassing quota accounting checks. Using instead ns_capable_noaudit() should fix this issue and prevent selinux audit messages. This also fix the remaining calls to has_capability_noaudit()	8.2	More Deta
CVE-2026-116244	When a pgAdmin 4 connection was not meant to use a Kerberos user's delegated credentials, pgAdmin removed KRB5CCNAME from its environment, so the Kerberos library fell back to the default credential cache, or a client keytab, of the operating-system account running pgAdmin. libpq then answered any server that asked for GSSAPI authentication with that account's ticket, whatever user name the pgAdmin user gave, so in server mode any user could connect as the service account's Kerberos principal; gssencmode=disable did not prevent it. On Windows, SSPI used the service account's logon in the same way. psql was also started with pgAdmin's environment, which could hold another user's credential cache while that user was connecting. The fix points KRB5CCNAME and KRB5_CLIENT_KTNAME at a file that cannot exist except while a Kerberos-authenticated user connects with Kerberos, and gives every other connection, psql and the utilities require_auth=!gss,!sspi and gssencmode=disable, checked on the final connection string. require_auth needs libpq 16 or later. This issue affects pgAdmin 4: before 9.19.	8.2	More Deta
CVE-2026-119050	Agno through 3.1.11 contains an unsafe reflection vulnerability in PandasTools that allows attackers to invoke arbitrary pandas functions by supplying model-controlled function names to getattr(). Attackers can use prompt injection to make the agent call pandas.read_pickle on attacker-controlled paths for code execution, or call other readers to read local files.	8.1	More Deta
CVE-2026-119419	CakePHP through 5.4.3 contains an sql injection vulnerability that allows attackers to inject SQL by supplying unvalidated collation values to StringExpression and IdentifierExpression. Attackers controlling a collation name passed to the constructor or setCollation() can append SQL after the unquoted COLLATE clause, affecting every database driver within the connection's privileges.	8.1	More Deta
CVE-2026-119418	CakePHP through 5.4.3 contains an sql injection vulnerability that allows attackers to inject SQL by supplying unvalidated frame offsets and directions to WindowExpression::range() and frame(). Attackers can pass crafted values through applications forwarding user input into the OVER clause to execute SQL with the database connection's privileges.	8.1	More Deta
CVE-2026-104317	IBM Langflow OSS 1.0.0 through 1.12.3 could allow a remote attacker who could reach the message broker to execute arbitrary code on the system due to the deserialization of untrusted data.	8.1	More Deta
CVE-2026-107018	Insecure permissions in Ghost Commander File Manager versionCode 479 allows unauthorized attackers to arbitrarily read and write files inside the commander's private storage.	8.1	More Deta
CVE-2026-90867	Improper access control in the Web Admin console of Progress Software WS_FTP Server versions prior to 2024.0.7 and 2025.0.4 on Windows could expose administrative functionality to remote authentication attempts.	8.1	More Deta
CVE-2026-85899	Use after free in Microsoft Edge (Chromium-based) allows an authorized attacker to elevate privileges over a network.	8.1	More Deta
CVE-2026-119129	ZITADEL 3.0.0 through 3.4.15 and 4.0.0 before 4.19.5 contains a missing authorization vulnerability in Login V2 that allows attackers to approve OAuth 2.0 device authorizations using a victim's existing session without consent. Attackers can send a signed-in user a link carrying the attacker's user code to obtain the victim's tokens, and can bypass project access settings via the OIDC device authorization API.	8.1	More Deta
CVE-2026-119127	ZITADEL 4.0.0 before 4.19.5 contains a host header injection vulnerability in the Login V2 UI that allows unauthenticated attackers to poison password-reset, invite, and email-verification links by supplying untrusted x-zitadel-public-host, x-zitadel-forward-host, or x-forwarded-host headers. Attackers knowing a victim's login name can point the links in genuine emails at their host, harvest the single-use codes when the links are opened, and take over accounts including instance administrators.	8.1	More Deta
CVE-2026-62967	ZTNET is a ZeroTier web UI for private controllers with multiuser and organization support. Prior to 0.8.0, any authenticated low-privilege user can permanently deactivate another account, including an administrator, through `POST /api/auth/user/invalidateUser`. In `src/pages/api/auth/user/invalidateUser.ts`, `getServerSession` checks only that a session exists and does not compare `session.user.id` with the client-supplied `userId`. Supplying a victim's `userId` and a `deviceId` for which no matching pair exists in `UserDevice` makes the handler set the target account's `isActive` to false. Login is then refused by `src/server/auth.ts` with `account-expired`. An attacker needs only a normal authenticated account and the victim's user ID, which may be obtainable from member lists, UI responses, logs, or other application metadata. This can lock administrators out, disrupt organization management, and deny access to any targeted user. This issue is fixed in version 0.8.0.	8.1	More Deta
CVE-2026-62989	Shopper is a Headless e-commerce Admin Panel. Prior to 2.10.0, the Variants Livewire component in `packages/admin/src/Livewire/Components/Products/Form/Variants.php` exposes `DeleteAction` and `DeleteBulkAction` without server-side authorization. An authenticated staff user with `edit_products` can access `/shopper/products/{id}/edit` and obtain the signed component state even without `delete_product_variants`. The `callTableAction` and `callTableBulkAction` paths then permanently delete individual or multiple variants without checking that dedicated permission. For variant products, this can destroy the sellable catalogue and disrupt storefront product pages, cart, and checkout. This issue is fixed in version 2.10.0.	8.1	More Deta
	LightSAML implements SAML 2.0 data model classes, XML serialization and deserialization, XML security, certificate support, and message bindings. Prior to 4.7.1 and 5.0.1, LightSAML and xmlseclibs disagree about which assertion an inbound SAML signature covers. `Response::deserialize` uses `manyElementsFromXml` to collect only direct-child `saml:Assertion` elements of `samlp:Response`, and `AssertionSignatureValidatorAction` validates their `ds:Signature` using an out-of-band trusted IdP credential resolved by Issuer, not a key from		

CVE-2026-63182	the document. `XMLSecurityDSig::validateReference()` removes the enveloped signature from the shared DOM, but `processRefNode()` resolves `Reference URI="#id"` document-wide through an XPath of the form `//*[@Id]` and takes `item(0)`, which need not be the assertion whose claims LightSAML consumes. An attacker who has captured one genuinely signed assertion, such as an earlier login response, can place its signature-stripped bytes earlier in `samlp:Extensions` and present a forged direct-child assertion with the same ID and copied genuine signature. Validation then covers the hidden genuine bytes while LightSAML surfaces unsigned attacker-controlled `Subject/NameID`, `Conditions`, and `Attributes`, enabling authentication bypass or privilege escalation even when signature validation is required. The behavior was confirmed in versions 5.0.0 and 4.6.1. This issue is fixed in versions 4.7.1 and 5.0.1.	8.1	More Deta
CVE-2026-117617	Jenkins 2.587 and earlier, LTS 2.580.1 and earlier checks for symbolic links in the path of an extracted file only before creating its parent directories, not immediately before writing it, and allows symbolic links in artifacts to replace existing files or empty directories, allowing attackers with Item/Configure permission to write files to arbitrary locations on the Jenkins controller file system.	8.1	More Deta
CVE-2026-118485	Axel Download Accelerator 2.17.14 and earlier performs URL percent-decoding (http_decode()) on the output filename after the URL has been parsed and the filename component extracted. This allows an attacker to embed %2e%2e%2f (URL-encoded ../) sequences in the URL path. These sequences survive the URL parser intact (they contain no literal / characters) but are decoded into directory traversal sequences before the output file is opened for writing. As a result, a crafted URL can cause axel to write downloaded content to arbitrary filesystem paths relative to the current working directory.	8.1	More Deta
CVE-2026-51903	SuperAGI v0.0.14 contains an improper access control vulnerability in get_agent_by_latest_execution in superagi/controllers/agent_execution.py. A remote authenticated attacker from one organization can retrieve latest execution and agent metadata for another organization's project through /agentexecutions/get/latest/agent/project/{project_id} by supplying a victim project_id.	8.1	More Deta
CVE-2026-61671	WeGIA is a web manager for charitable institutions. Prior to the advisory's stated patched version 3.8.7, the `/controle/control.php` dispatch endpoint accepts attacker-controlled `nomeClasse`, `metodo`, and record identifier parameters through `extract($_REQUEST)`, including id, `idatendido`, `idInterno`, and `id_funcionario`, while the affected Controle CRUD methods do not verify record ownership. Any authenticated user can view, modify, or delete another user's records, exposing CPF, RG, addresses, medical records, financial data, and employee records. `AtendidoControle` lacks ownership checks on alterar, excluir, `listarUm`, `alterarInfPessoal`, `alterarDocumentacao`, `alterarImagem`, `alterarEndereco`, and `alterarStatus`; `InternoControle` lacks them on incluir, alterar, excluir, `listarUm`, `listarTodos`, and `listarCpf`. `FuncionarioControle` lacks ownership checks on `alterarInfPessoal`, `alterarEndereco`, `alterarDocumentacao`, `alterarImagem`, `alterarCargaHoraria`, and excluir; `VoluntarioControle` lacks them on `alterarInfPessoal`, `alterarEndereco`, `alterarDetalhes`, `alterarImagem`, and excluir. `AtendidoControle` and `InternoControle` additionally lack CSRF validation, allowing a malicious page visited by an authenticated victim to perform state-changing operations using the victim's session. `FuncionarioControle` and `VoluntarioControle` have per-method CSRF checks, but those checks do not prevent the object-authorization bypass. The advisory identifies version 3.8.7 as patched.	8.1	More Deta
CVE-2026-109411	An access control bypass flaw was identified in Samba's vfs_ceph_rgw module in it's openat() function. An authenticated user can bypass access controls to read or overwrite restricted files on shares configured with the experimental vfs_ceph_rgw module. When a client requests an existing file using mismatched character casing, the module fails to perform a case-insensitive lookup correctly, causing the server to treat the operation as creating a new file. As a result, the server skips standard permission checks on the existing file, allowing the attacker to access or overwrite sensitive data owned by other users.	8.1	More Deta
CVE-2026-115346	The Avada | Website Builder For WordPress & WooCommerce theme for WordPress is vulnerable to Arbitrary File Upload in versions up to, and including, 7.16.2 via the convert_palette_images_to_truecolor() function. This is due to insufficient file type validation before processing uploaded files. This makes it possible for unauthenticated attackers to upload files that may be executable, which makes remote code execution possible.	8.1	More Deta
CVE-2026-118633	A path traversal vulnerability allows a remote unauthenticated attacker to execute arbitrary code as root in Sophos UTM (all versions) after winning a race condition by sustaining repeated attacks for a few minutes when the email proxy is used with scanning enabled. Sophos UTM is end-of-life and the patch must be installed manually.	8.1	More Deta
CVE-2026-84725	when EAP runs with -secmgr, the openjdk-orb's JDKBridge honours attacker-supplied CDR codebase URLs during object unmarshalling on :3528, allowing an unauthenticated attacker to load and instantiate arbitrary classes from a remote URL in the server JVM before EJB security interceptors run.	8.1	More Deta
CVE-2026-61804	myTinyWMS is a free, open-source warehouse management system. Prior to version 1.6.4, `Product (Artikel)` and `Category` management store the `name` parameter without adequate backend sanitization and render raw database strings through unescaped Blade output in dynamic table cells, including `article/index.blade.php` and `category/index.blade.php`. An authenticated attacker can save malicious input through product creation or category forms. When another user, including a worker or administrator, opens the corresponding product sheet, category listing or dashboard, the stored JavaScript executes in that user's browser context. This can enable cross-user script execution, session theft and administrative takeover. This issue is fixed in version 1.6.4.	8.1	More Deta
CVE-2026-118375	llama.cpp b8841 before b11865 contains an out-of-bounds write vulnerability in the ggml-rpc RDMA transport rdma_recv() function that allows unauthenticated peers to overflow the rpc-server stack. Attackers advertising RDMA capabilities in the HELLO message can send up to 256 KiB into a 1-byte stack variable in rpc_serve_client(), crashing the server or potentially executing code.	8.1	More Deta
CVE-2026-116238	In server mode pgAdmin 4 locks an internal account after MAX_LOGIN_ATTEMPTS failed logins (3 by default). The limit could be bypassed, giving an unauthenticated attacker an unlimited number of password guesses against any internal account, including the administrator's, in the default configuration: - Flask-Security registers its own views next to pgAdmin's. A login submitted to its /login view was checked and logged in without pgAdmin's failed login count or lock. Its /verify view checked a signed-in user's password without limit, its /change view changed a password without pgAdmin's change password permission or re-encrypting the user's saved server passwords, and its /reset views sent and applied password resets for accounts that are not internal or are locked. - The internal account was looked up by its exact username, while the login form matches the email ignoring case, so a login with the username typed in another case was neither counted nor checked for the lock. - With LDAP or webserver authentication also configured, a wrong internal password was never counted, and with Kerberos or webserver authentication configured a guess could be answered without being counted. In addition, where accounts from different authentication sources share an email address, a password reset could be sent for, or applied to, an account from another source, and the About box showed the server configuration to a user whose email was that of an administrator's account. The fix refuses submissions to Flask-Security's own views, counts every failed internal login however the username is typed and whatever other sources are configured, no longer lets a login that posts a password fall back to an authentication source that does not check it, and locks only internal authentication. Password resets and the About box act only on the user's own internal account. Desktop mode is not affected. This issue affects pgAdmin 4: before 9.19.	8.1	More Deta
CVE-2026-85749	MailWatch for MailScanner is a web-based front-end to MailScanner. Prior to 1.2.27, any authenticated MailWatch user, including the U/user, D/domain-admin, and H/host roles, can release to inbox or permanently delete the quarantined mail of any other user or domain by supplying an arbitrary message `id` to `mailscanner/quarantine_action.php`. The action path calls `quarantine_list_items()` in `mailscanner/functions.php`, which selects from `maillog` by the supplied identifier without the per-role `global_filter` applied by listing and read views. The action requires a valid session and CSRF token, but the caller can submit a token from the caller's own session; ownership of the requested message is never checked. Message identifiers are enumerable, allowing a low-privilege user to invoke `quarantine_release()` or `quarantine_delete()` for other users' or domains' quarantined messages, force-delivering mail held by the quarantine or permanently deleting it. This issue is fixed in version 1.2.27.	8.1	More Deta

CVE-2026-96228	SSL Wireless SMS Notification for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 3.8.1. The public final_login_ajax_action handler resolves a user and issues an authenticated session by matching the wp_sslcare_otp table on only the attacker-supplied phone and cap_data, without verifying the SMS OTP or any server-side single-use state. Because cap_data was chosen by the attacker in the public otp_login_ajax_action step (which stores the row before sending the SMS), the finalize step trivially matches and the user is looked up solely by the sslcare_login_phone meta. This makes it possible for unauthenticated attackers who know a phone-linked user's number to take over that account.	8.1	More Deta
CVE-2026-117619	Jenkins 2.587 and earlier, LTS 2.580.1 and earlier allows requests authenticated using HTTP Basic authentication, including with an API token, to obtain a "remember me" cookie, allowing attackers who have obtained a user's API token to retain access to Jenkins using a "remember me" cookie after the API token is revoked or expires.	8.1	More Deta
CVE-2026-117618	In Jenkins 2.587 and earlier, LTS 2.580.1 and earlier, the HTTP endpoint for creating the first user account does not check whether the setup wizard has been completed, resulting in a race condition that allows unauthenticated attackers to create an administrator account while the initial user account is being replaced.	8.1	More Deta
CVE-2026-93851	Mattermost versions 11.9.x <= 11.9.1, 11.8.x <= 11.8.5, 11.7.x <= 11.7.10 fail to validate the target post ID in the Agents plugin's mention reminder component, which allows an authenticated user who can post in a channel visible to a system administrator to cause the administrator's browser to send an unintended API request, resulting in replacement of an installed plugin and code execution on the server, via a crafted post containing a forged mention reminder that the administrator clicks. Mattermost Advisory ID: MMSA-2026-00742	8.0	More Deta
CVE-2026-118696	In JetBrains IntelliJ IDEA, PyCharm, PhpStorm, RubyMine and WebStorm before 2026.3, 2026.2.4, 2026.1.5.1, and 2025.3.6.2; GoLand before 2026.3, 2026.2.4, 2026.1.5.1, and 2025.3.5.2; Rider before 2026.3, 2026.2.4, 2026.1.5.3, and 2025.3.5.3; CLion before 2026.3, 2026.2.4.1, 2026.1.5.2, and 2025.3.6.3; DataGrip before 2026.3, 2026.2.6.1, 2026.1.4.1, and 2025.3.6.1; RustRover before 2026.3, 2026.2.5, 2026.1.4.1, and 2025.3.7.1; DataSpell before 2026.1.3.1 and 2025.3.3.1, the embedded browser trusted revoked intermediate certificates	8.0	More Deta
CVE-2026-91917	Dell OpenManage Enterprise, versions prior to 4.8.0, contains an Improper Input Validation vulnerability. A low privileged attacker with adjacent network access could potentially exploit this vulnerability, leading to Code execution.	8.0	More Deta
CVE-2026-119287	Zuke is a code-first, strongly typed build automation system for Deno. Prior to 1.51.0, the @zuke/core MCP registry mode accepts command-form registry descriptors without applying the ZUKE_REGISTRY_LAUNCH_HOSTS authorization enforced for remote module descriptors. When zuke mcp --registry --allow-run reads a registry writable by another party and a run-capable caller invokes the affected tool, the registry writer can choose the program and arguments executed with the operator's environment and workspace access. The --allow-run and --protect name globs do not contain the issue because the descriptor supplies those names, and the optional destructive confirmation displays a description controlled by the same writer. The local default registry populated only through zuke register is not affected because that command writes module-form descriptors. This issue is fixed in version 1.51.0.	8.0	More Deta
CVE-2026-62958	libriscv is a RISC-V sandbox and emulator. Prior to 1.18, a crafted ELF binary can cause out-of-bounds reads in the host emulator. `Memory<W>::binary_loader` checks `PT_LOAD` program-header bounds, but `Memory<W>::serialize_execute_segment` trusts section-header `sh_offset` and `sh_size` when locating `.text` without verifying the file range against `m_binary.size()`; `Memory<W>::lookup()` has a similar section-table problem. Malformed `.text` or `.symtab` offsets can therefore bypass the program-header checks and point outside the binary buffer, crashing rvlinux. With suitable memory layout or integer overflow, out-of-buffer host heap memory may instead be mapped into the guest by `create_execute_segment()`, potentially exposing host memory. The reported reproducer demonstrates a host SIGSEGV, while memory disclosure through grooming is described as possible rather than demonstrated. This issue is fixed in version 1.18.	7.9	More Deta
CVE-2026-104615	A security vulnerability was discovered in SUSE Rancher Fleet's cluster registration flow, in Fleet versions before 0.12, 0.13.0 up to 0.13.17, 0.14.0 up to 0.14.12, 0.15.0 up t o 0.15.17 and 0.16.0 up to 0.16.3. The cluster identity claimed by a registration request was accepted without being bound to the registration token that the request was made with. As a result, a registration request could be associated with a managed cluster that was originally registered with a different registration token.	7.9	More Deta
CVE-2026-118688	wasmtime-wasi in Wasmtime before 36.0.18, 37.0.0 before 48.0.6, and 49.0.0 before 49.0.3 re-appends a trailing slash to rename source paths, causing renameat on macOS and FreeBSD hosts to follow directory symlinks. A guest with sandbox write access can rename a relative symlink such as "up/" to move host directories into its sandbox and read or write them.	7.9	More Deta
CVE-2026-93522	A heap buffer overflow caused by mismatched size usage in CopyArea CPU-to-FBO path in X.Org X Server before 21.1.15 and XWayland before 24.1.14 could be used by authenticated X clients to crash or potentially execute code in the X server context.	7.8	More Deta
CVE-2026-99163	In the Linux kernel, the following vulnerability has been resolved: tracing/histograms: Reject non-stacktrace fields for synthetic stacktrace fields In check_synth_field(), when a synthetic event field is a stacktrace (field->is_stack) and the histogram field is not a "long[" stacktrace array, validation falls through to the generic size and signedness comparison. Because parse_synth_field() sets a stacktrace field's type to "__data_loc unsigned long[]", its size is sizeof(u64) and synth_field_signed() marks it as signed. Consequently, any 8-byte signed scalar histogram field passes the fallback check, and its scalar value is subsequently dereferenced as a kernel stacktrace pointer in get_field_size() and trace_stack(). Furthermore, checking strstr(hist_field->type, "long[") is insufficient because tracepoint fields defined with __bitmask() or __rel_bitmask() also have type "__data_loc unsigned long[]" or "__rel_loc unsigned long[]", whilst create_hist_field() treats them as 4-byte scalar values without HIST_FIELD_FL_STACKTRACE. Propagate HIST_FIELD_FL_STACKTRACE to variable references and field variables (whilst excluding variable aliases from per-element stacktrace capture), and reject any mismatch between HIST_FIELD_FL_STACKTRACE and field->is_stack in check_synth_field().	7.8	More Deta
CVE-2026-99213	In the Linux kernel, the following vulnerability has been resolved: vsock: treat TCP_CLOSING as once-established Handle the TCP_ESTABLISHED -> TCP_CLOSING transition on OP_RST, which can race with the connect loop. Immediately break and return 0 on ESTABLISHED/CLOSING. The return value of connect() should reflect what happened up to the point the connection was established or failed. Events that occur afterwards must not affect it. E.g. even if OP_RW has already set sk_err, connect() should still return 0, not ENOBUFS because of it. Adapt the inaccurate comment above signal_pending(). Resetting a socket that is still present in connected_table can lead to memory corruption. The reporter noted lost transports for in-flight skbs, and I have reproduced crashes caused by re-insertion into connected_table. list_add double add: new=, prev=, next=. kernel BUG at lib/list_debug.c:35! Oops: invalid opcode: 0000 [#1] SMP KASAN NOPTI Workqueue: vsock-loopback vsock_loopback_work RIP: 0010:__list_add_valid_or_report+0x11f/0x130 Call Trace: vsock_insert_connected.cold+0xe/0x13 virtio_transport_recv_pkt+0x10e9/0x1460 vsock_loopback_work+0x305/0x480 process_one_work+0xe4c/0x1560 worker_thread+0x4f1/0xd60 kthread+0x36e/0x470 ret_from_fork+0x47b/0x6b0 ret_from_fork_asm+0x1a/0x30 This fix is supplementary to commit 002541ef650b ("vsock: Ignore signal/timeout on connect() if already established"). Details under Link.	7.8	More Deta
CVE-2026-93521	A buffer overflow in RandR ChangeProviderProperty requests in X.Org X Server before 2.1.25 and XWayland before 24.4.14 could be used by authenticated X clients to crash or execute code within the X server context.	7.8	More Deta
	In the Linux kernel, the following vulnerability has been resolved: pipe: preserve existing fasync readers on writer setup failure F_SETFL and FIOASYNC decide whether to invoke ->fasync() before pipe_fasync() takes pipe->mutex. Two enables of one O_RDWR FIFO can therefore both		

CVE-2026-99203	enter the callback. fasync_helper() allocates before checking for an existing entry. If the first enable installs both entries, a second enable can update the reader entry and then fail the allocation for the writer entry. The error path removes the pre-existing reader entry, clearing FASYNC while the writer entry remains registered. __fput() then skips ->fasync(), so a later pipe notification can dereference the freed file or its f_owner. An unprivileged memory-pressure reproducer triggers a KASAN slab-use-after-free in send_sigio() through this path. Keep the reader helper's result and undo the registration only if this call added it. The pipe mutex serializes changes to both lists, so a failed new registration still removes its reader, while a failed duplicate preserves the existing registrations and FASYNC. Successful duplicate enables continue to update fa_fd as before.	7.8	More Deta
CVE-2026-99109	In the Linux kernel, the following vulnerability has been resolved: smb: client: reject SetEA requests that do not fit the request buffer CIFSSMBSetEA() copies the caller's extended attribute value into the SMB request buffer without checking that it fits. The requirement is stated in the source but was never implemented: /*BB add length check to see if it would fit in negotiated SMB buffer size BB */ /* if (ea_value_len > buffer_size - 512 (enough for header)) */ if (ea_value_len) memcpy(parm_data->list.name + name_len + 1, ea_value, ea_value_len); The only bound applied on the way in is in cifs_xattr_set(): #define MAX_EA_VALUE_SIZE CIFSMaxBufSize ... if (size > MAX_EA_VALUE_SIZE) CIFSMaxBufSize is the full payload capacity of the buffer, so a value of exactly that size leaves no room for the SMB header, the TRANS2 parameter block, the fealist header and the EA name that are written ahead of it in the same object. SendReceive() already enforces the correct limit on this very length: if (in_len > CIFSMaxBufSize + MAX_CIFS_HDR_SIZE) but it is called after the copy has taken place. An unprivileged setxattr(2) on an SMB1 mount with a 250-byte name and a 16384-byte value writes 16384 bytes starting 345 bytes into a 16588-byte cifs_request object, ending 141 bytes past it: BUG: KASAN: slab-out-of-bounds in CIFSSMBSetEA+0xabc/0xde0 Write of size 16384 at addr ffff888003aa0159 by task init/68 __asan_memcpy+0x3c/0x60 CIFSSMBSetEA+0xabc/0xde0 cifs_xattr_set+0xd3a/0xff0 __vfs_setxattr+0x13e/0x1a0 The buggy address is located 345 bytes inside of allocated 16588-byte region Apply SendReceive()'s limit to the assembled request before the copy rather than after it, and widen the byte counters so the sum cannot wrap before it is tested. byte_count is also tested against U16_MAX, because it is stored in the 16-bit pSMB->ByteCount. That becomes reachable when CIFSMaxBufSize is raised at module load, where it may be set as high as 1024*127: with a 5-byte EA name and a 65521-byte value, count is exactly U16_MAX while byte_count is 65556, and cpu_to_le16() would truncate it to 20 and transmit a frame whose ByteCount does not match its length. Testing byte_count covers count as well, since byte_count is the larger of the two and count's only 16-bit consumer is written after this point. check_add_overflow() is evaluated first so that total_len is assigned before it is reported.	7.8	More Deta
CVE-2026-112357	GFI KerioConnect (Kerio Connect) Outlook Connector (Offline Edition), 'KOFF', before 10.0.9 Patch 2 contains a local privilege escalation vulnerability caused by weak installer permissions that leave the product directory writable by the built-in Users group. A local non-administrative attacker can replace the searchd.exe service binary used by the bundled KOFFIndexingService, which runs as LocalSystem, to execute arbitrary code with NT AUTHORITY\SYSTEM privileges upon the next service start or reboot.	7.8	More Deta
CVE-2026-59176	Functype is a family of TypeScript functional programming libraries. Prior to 1.4.4, the `set_functype_version` MCP tool in `functype-mcp-server` accepts an unconstrained `version` string using only `z.string()` validation in `packages/mcp-server/src/index.ts` and interpolates it into `functype@<version>` for `pnpm add`. Package-alias syntaxes such as `file:`, `npm:`, URLs, or paths can cause an arbitrary local or remote package to be installed as functype. Immediately afterward, `initDocsData(true)` in `packages/mcp-server/src/lib/docs/data.ts` resolves `functype/cli` and dynamically imports the newly installed module, executing attacker-controlled JavaScript with the MCP server process's privileges. Any MCP client able to send a `tools/call` request invoking the tool can exploit the flaw; the tool is enabled by default without authentication in `stdio` mode. A connected AI assistant susceptible to indirect prompt injection can also be induced to invoke it from a malicious document or web page. In non-default `TRANSPORT_TYPE=httpStream` deployments, a network-accessible attacker does not require local access. Successful execution can read process secrets, modify files, or terminate the server. This issue is fixed in `version` 1.4.4.	7.8	More Deta
CVE-2026-59172	Joker is a small Clojure interpreter, linter and formatter written in Go. Prior to 1.8.2, `joker --lint <file>` walks upward from the linted file to locate a `.jokerd/` directory and executes matching `linter.*` files before linting. Those files contain executable Joker/Clojure code, so linting a file inside an untrusted repository can execute repository-supplied code with the linter user's privileges. Editor integrations and CI jobs that automatically lint checked-out source can trigger this behavior. The patch stops executing project-local linter customizations and loads executable customization only from the user's home directory. This issue is fixed in version 1.8.2.	7.8	More Deta
CVE-2026-99180	In the Linux kernel, the following vulnerability has been resolved: unicode: free the map after a grace period generic_ci_d_hash() and generic_ci_d_compare() read sb->s_encoding and dereference the unicode map while a pathwalk in rcu mode holds nothing but rcu_read_lock(). The filesystems that use them, ext4, f2fs and tmpfs, drop the map with utf8_unload() from ->put_super(), which runs when the last reference to the mount goes away. A lookup that is still inside such a filesystem at that point reads a freed map. With a pathwalk held up in utf8_casefold_hash() while the last reference to a casefolded tmpfs goes away: BUG: KASAN: slab-use-after-free in utf8nlookup+0x74c/0x950 Read of size 8 at addr ff110001030fe658 by task walker/98 Call Trace: <TASK> utf8nlookup+0x74c/0x950 utf8byte+0x160/0x1560 utf8_casefold_hash+0x167/0x230 generic_ci_d_hash+0xdd/0x1c0 link_path_walk+0x11ad/0x1d30 path_lookupat+0x63/0xb00 filename_lookup+0x1f1/0x5b0 vfs_statx+0xd7/0x3b0 [...] Allocated by task 94: __kmalloc_cache_noprof+0x249/0x560 utf8_load+0x4e/0x570 shmem_parse_opt_casefold.isra.0+0x92/0x270 [...] Freed by task 97: kfree+0x1db/0x5b0 shmem_put_super+0x72/0x170 generic_shutdown_super+0x14c/0x530 kill_anon_super+0x3a/0x60 deactivate_locked_super+0x9c/0xf0 cleanup_mnt+0x9f/0x130 So far that has been hard to hit. umount(2) waits for a grace period in namespace_unlock() before it drops the mount, so only a mount whose last reference goes away elsewhere, like the close of a file or a chdir out of a lazily unmounted directory, can race a walker. So it is reachable. Delay the free until a grace period has passed. The map and the data table it holds a reference to then outlive any pathwalk that found the superblock before the mount went away. The reference on the data table module is dropped from the rcu callback as well. utf8-core is built in whenever CONFIG_UNICODE is set, so there is no module exit that would have to wait for the callbacks. Overlayfs points the s_encoding of an overlay at the map of its first layer without taking a reference of its own. That stays correct. The layer is held by the overlay, so its map is dropped only after the overlay is gone.	7.8	More Deta
CVE-2026-118753	FreeImage through 3.18.0 and the danoli3 FreeImage fork before 3.19.25 contain a heap buffer overflow vulnerability in PluginGIF.cpp that allows attackers to write past the canvas allocation via unclipped GIF frame rectangles. Attackers can craft a GIF whose frame left plus width exceeds the logical screen width, causing GifPlaybackCompositeFrame() and GifPlaybackFillRect() to corrupt heap memory when loaded with GIF_PLAYBACK.	7.8	More Deta
CVE-2026-93520	A heap buffer overflow caused by mismatching size calculations between XkbAllocNames and ChangeKeycodeRange in X.org X server before 2.1.25 and XWayland before 24.1.14 could be used by authenticated X clients to crash or potentially execute code in X server context.	7.8	More Deta
CVE-2026-118752	FreeImage through 3.18.0 and the danoli3 FreeImage fork before 3.19.22 contain a heap buffer overflow vulnerability in the PBM RLE decoder of PluginIFF.cpp that lacks bounds checks on ByteRun1 runs. Attackers can supply a crafted IFF/LBM PBM file with runs straddling scanline ends to write up to 127 controlled bytes past the heap-allocated bitmap.	7.8	More Deta
CVE-2026-99107	In the Linux kernel, the following vulnerability has been resolved: ntfs: fix incorrect MFT record pointer passed to ntfs_attr_record_resize ntfs_new_attr_flags() passes the wrong MFT record to ntfs_attr_record_resize(). When the attribute is in an extent record, ctx->mrec points to the extent but the function receives the base record pointer m, causing incorrect size calculations in memmove. Fix by passing ctx->mrec (the actual MFT record containing the attribute) instead of m (the base MFT record) to ntfs_attr_record_resize().	7.8	More Deta
	In the Linux kernel, the following vulnerability has been resolved: eventfs: Free the eventfs_inode after an rcu grace period too tracefs_d_revalidate() reads ->is_freed of the eventfs_inode that dentry->d_fsdata points to, and ->d_revalidate() is called in rcu pathwalk mode with nothing but rcu_read_lock() held. The dentry itself stays around for such a walker, but tracefs_d_release() drops its reference to the		

CVE-2026-99173	eventfs_inode when the dentry is killed, and release_ei() then frees it after a grace period of eventfs_srcu. An SRCU grace period doesn't wait for rcu_read_lock() sections, so the walker can read an eventfs_inode that is already gone. With a pathwalk held up in tracefs_d_revalidate() while the dentry goes away: BUG: KASAN: slab-use-after-free in tracefs_d_revalidate+0x76/0x90 Read of size 1 at addr ff1100010152d8d0 by task walker/97 Call Trace: <TASK> tracefs_d_revalidate+0x76/0x90 lookup_fast+0x320/0x640 path_lookupat+0x160/0xb00 filename_lookup+0x1f1/0x5b0 vfs_statx+0xd7/0x3b0 vfs_fstatat+0x4d/0x90 __do_sys_newfstatat+0xa0/0x100 do_syscall_64+0x10e/0x5e0 entry_SYSCALL_64_after_hwframe+0x77/0x7f [...] Allocated by task 1: __kmalloc_cache_noprof+0x249/0x560 eventfs_create_dir+0x7a/0x590 event_create_dir+0x2fb/0xcf0 trace_add_event_call+0xbf/0x150 [...] Freed by task 11: kfree+0x1db/0x5b0 srcu_invoke_callbacks+0x3a3/0x620 process_one_work+0x937/0x1810 worker_thread+0x4f1/0xd60 Before commit 8e556432477e ("eventfs: Use SRCU for freeing eventfs_inodes") release_ei() used call_rcu(), which covered the walker, while eventfs_iterate() needs the SRCU grace period. Wait for both and chain call_rcu() from the SRCU callback.	7.8	More Deta
CVE-2026-99177	In the Linux kernel, the following vulnerability has been resolved: KVM: SEV: Fix page dirtying in sev_gmem_post_populate() set_page_dirty() requires that the caller holds some kind of lock to ensure that the page's mapping does not concurrently go away. That is not the case for a random page we got from get_user_pages_fast(), so use set_page_dirty_lock(). [sean: tag for stable]	7.8	More Deta
CVE-2026-93518	An integer truncation issue in XkbResizeKeyType() that could lead to a heap buffer overflow by authenticated X clients in X.org X server before 21.1.25 and XWayland before 24.1.14 could be exploited for crashes or potential code execution in the X server.	7.8	More Deta
CVE-2026-99143	In the Linux kernel, the following vulnerability has been resolved: tracing: Keep the predicate limit separate from program capacity predicate_parse() adds two to nr_preds to reserve the terminal TRUE and FALSE entries. It also uses that increased value as the limit for parsed predicates. If the initial count is smaller than the number actually parsed, the program can fill the allocation and subsequent accesses can go past its end. Keep nr_preds as the predicate limit and use a separate value for the allocation size. This leaves space for both terminal entries and a zeroed entry when parsing stops at the limit.	7.8	More Deta
CVE-2026-93519	A buffer overflow when handling pointer barriers in the XFIXES extension in X.Org X server before 21.1.25 and XWayland before 24.1.14 could be used by authenticated X clients to crash or potentially execute code in X server context.	7.8	More Deta
CVE-2026-82961	The GPIO syscall handlers in drivers/gpio/gpio_handlers.c did not validate the pin argument supplied by a user-mode caller. z_vrfy_gpio_pin_configure(), z_vrfy_gpio_pin_get_config() and z_vrfy_gpio_pin_interrupt_configure() verified only the device object (K_SYSCALL_DRIVER_GPIO() / K_SYSCALL_OBJ()) and then passed the caller-supplied gpio_pin_t straight through to z_impl_gpio_pin_*() and on to the driver. The only pin check in include/zephyr/drivers/gpio.h was __ASSERT(gpio_port_pin_is_supported(cfg->port_pin_mask, pin), ...), which compiles to nothing unless CONFIG_ASSERT is enabled, so in a production build no check existed at all. GPIO drivers use pin as a shift count and as an array index on the documented assumption that it is a pin the controller supports. On STM32, for example, gpio_stm32_pin_interrupt_configure() turns pin into an EXTI line and stm32_gpio_intc_set_irq_callback() writes data->cb[line_num].cb and data->cb[line_num].data into a NUM_EXTI_LINES-entry array (default 16) in drivers/interrupt_controller/intc_gpio_stm32.c, guarded only by a compiled-out __ASSERT_NO_MSG(); the same function then reads exti_irq_table[line_num] and calls irq_enable() on the result. Other controllers index fixed-size per-pin configuration tables the same way — drivers/gpio/gpio_ite_it8xxx2_v2.c reads an MMIO base pointer out of wuc_base[8] with the caller's pin and performs a read-modify-write through it. The issue is reachable only in builds with CONFIG_USERSPACE=y (the file is compiled under that symbol), by a user-mode thread that has been granted access to a GPIO device object. Such a grant is intended to authorize control of that port's pins; the missing validation instead lets the thread drive a supervisor-mode out-of-bounds write of a function pointer and an associated void * past a kernel .bss array, and out-of-bounds reads that feed irq_enable() and MMIO accesses — an escape from the user-mode sandbox that can lead to kernel memory corruption, arbitrary code execution, or a crash. The fix validates pin against the controller's gpio_driver_config.port_pin_mask with gpio_port_pin_is_supported() in every pin-taking z_vrfy_ handler and returns -EINVAL otherwise, complemented by an unconditional pin >= GPIO_MAX_PINS_PER_PORT range check added to the shared z_impl_gpio_pin_*() inlines.	7.8	More Deta
CVE-2026-99167	In the Linux kernel, the following vulnerability has been resolved: net/sched: fix use-after-free in __tcf_action_put() __tcf_action_put() decrements the reference count before decrementing the binding count. Another thread can free the action between these operations, causing the binding-count update to access freed memory. KASAN reports it as: BUG: KASAN: slab-use-after-free in __tcf_action_put+0x327/0x340 Write of size 4 at addr ff11000000d46420 by task tc-put-pause/64 Hold the action IDR mutex across both counter updates and IDR removal, keeping cleanup outside the lock.	7.8	More Deta
CVE-2026-99156	In the Linux kernel, the following vulnerability has been resolved: scsi: st: Fix use-after-free race between st_remove() and st_open() st_remove() drops the probe reference on the scsi_tape with kref_put() and only afterwards removes its index from st_index_idr. If that was the last reference, scsi_tape_release() frees the structure while it is still published in the idr. scsi_tape_get(), called from st_open(), looks up the tape in st_index_idr and takes a reference under st_ref_mutex and st_index_lock. remove_cdevs() does not wait for opens that are already past chrdev_open(), so an open that is blocked on st_ref_mutex while st_remove() holds it can take the mutex as soon as st_remove() drops it, find the freed tpnt in the idr and call kref_get() on it: BUG: KASAN: slab-use-after-free in st_open Write of size 4 ... st_open (drivers/scsi/st.c:254 drivers/scsi/st.c:1291) chrdev_open ... Freed by task ...: kfree st_remove (drivers/scsi/st.c:4512) Remove the index from the idr before dropping the reference, all under st_ref_mutex. A concurrent scsi_tape_get() now either runs first and holds a valid reference that keeps the tape alive, or runs afterwards and finds nothing, so st_open() fails with -ENXIO. This restores the ordering st_remove() had before the conversion to st_index_idr, where the tape was unpublished from scsi_tapes[] before the final kref_put().	7.8	More Deta
CVE-2026-99164	In the Linux kernel, the following vulnerability has been resolved: spi: imx: fix slab corruption from undersized DMA bounce buffers Since commit faa8e404ad8e ("spi: imx: support dynamic burst length for ECSPI DMA mode"), the driver allocates its private DMA TX/RX buffers with kzalloc(dma_len), where dma_len is only rounded up to 4 bytes, but maps, syncs and unmaps them with DMA_CACHE_ALIGNED_LEN(dma_len), i.e. rounded up to the cache line size. As a result, the DMA API operates on memory beyond the end of the allocation. This was observed on a custom i.MX8MP platform with an mcp251xfd CAN controller under heavy RPMSG load, as a series of refcount_t warnings triggered from rpmsg_recv_done() in virtio_rpmsg_bus: refcount_t: addition on 0; use-after-free. refcount_t: underflow; use-after-free. refcount_t: saturated; leaking memory. Leading finally to an "Unable to handle kernel paging request" oops. Reproducing this problem took between 30 minutes and roughly 30 hours under the same workload. Hardware watchpoints on the refcount of a struct rpmsg_endpoint showed it was overwritten from 2 to 1 by __pi_memcpy_generic() in the irq/155-spi2.0 thread. Additionally it was found that a "normal" rpmsg_recv_done() took 11µs +/-2µs from its kref_get to kref_put. In the error case the same sequence took about 215µs +/-10µs. Based on this, an LLM was used to identify the size mismatch fixed here. Allocate the buffers with DMA_CACHE_ALIGNED_LEN(dma_len) so they cover the full mapped length, and use the same length for dma_sync_single_for_cpu() to stay consistent with map and unmap. With this patch applied, the same workload ran for more than 200 hours without the problem reproducing.	7.8	More Deta
CVE-2026-93523	A heap buffer overflow caused by a XIPassiveUngrabDevice request with an out-of-range modifier value in X.Org X Server before 21.1.15 and XWayland before 24.1.14 could be used by authenticated X clients to crash or potentially execute code in X server context.	7.8	More Deta
	In the Linux kernel, the following vulnerability has been resolved: net: bridge: mcast: don't truncate the port group walk on teardown __br_multicast_disable_port_ctx() and br_multicast_del_port() walk port->mglist with hlist_for_each_entry_safe(). However, br_multicast_find_del_pg() can also delete other entries from the same list through br_multicast_fwd_src_remove() or __fwd_del_star_excl(). If such an entry is the iterator's saved next node, hlist_del_init() clears its ->next and terminates the walk early. The reproducer triggers this in both		

CVE-2026-99117	teardown walks, leaving port groups in the bridge mdb with a dangling ->key.port after del_nbp() frees the port: BUG: KASAN: slab-use-after-free in __mdb_fill_info+0x1191/0x1320 __mdb_fill_info+0x1191/0x1320 br_mdb_dump+0x594/0xe40 rtnl_mdb_dump+0x1cf/0x5d0 Use hlist_del_init_rcu() to unlink the group while preserving ->next. br_multicast_del_pg() and the teardown walks run under br->multicast_lock. The GC worker must acquire the same lock before detaching the group for destruction, so the node remains alive while the walk uses the preserved pointer. Preserving ->next means a walk can now reach a group that an earlier iteration already deleted as a side effect. That group is off mp->ports, so br_multicast_find_del_pg() would fall through its port scan and hit the trailing WARN_ON(1). Skip such groups at the top of that helper: a port group is put on port->mglist when it is created and only unlinked when it is deleted, so hlist_unhashed() identifies exactly this case.	7.8	More Deta
CVE-2026-119719	Blender before 4.5.15 and 5.x before 5.2.3 contains a heap buffer overflow vulnerability in the blend file thumbnail extractor caused by 32-bit integer overflow in thumb_data_vertical_flip(). Attackers can craft a .blend file with malicious TEST block dimensions that trigger an out-of-bounds write when blender-thumbnailer or the Windows shell extension previews it, causing crashes or code execution.	7.8	More Deta
CVE-2026-104061	Scribus before 1.6.7 and 1.7.x before 1.7.4 contains a heap out-of-bounds write vulnerability in the scimgdataloader_psd loader that uses unchecked PSD file values as lookup array indexes. Attackers can convince users to place or import a crafted PSD file to corrupt heap memory, causing crashes and potentially code execution as the user.	7.8	More Deta
CVE-2026-119374	SQLite before 3.54.0 built with FTS5 contains a heap buffer overflow in fts5DoSecureDelete() that allows attackers to write past the leaf page buffer via crafted footer key offsets. Attackers can supply a database file with a corrupted FTS5 index that, when deleted from with secure-delete enabled, corrupts heap memory and crashes the application.	7.8	More Deta
CVE-2026-119379	SQLite before 3.54.0 built with the session extension contains a heap buffer overflow vulnerability in sqlite3changeset_apply() that allows attackers to corrupt heap memory by supplying crafted changesets. Attackers can repeat a table name in a second changeset block with a larger column count, causing sessionUpdateFind() to memset past the undersized aUpdateMask allocation.	7.8	More Deta
CVE-2026-104067	Scribus before 1.6.7 and 1.7.x before 1.7.4 contains an out-of-bounds memory access vulnerability in the importsvm plugin that fails to verify bitmap and transparency mask dimensions match. Attackers can supply a crafted SVM file with mismatched mask dimensions to trigger heap reads and writes, causing crashes or code execution as the user.	7.8	More Deta
CVE-2026-119528	A flaw was found in GIMP. The PSD plug-in’s image resource header loader uses an incorrect destination size when copying a converted resource name into a fixed stack buffer. Opening a crafted PSD file can cause a stack-based buffer overflow, leading to a crash and potentially arbitrary code execution.	7.8	More Deta
CVE-2026-115805	Improper handling of local filesystem paths in Rapid7 Insight Agent on Linux and macOS may allow authenticated local users to gain elevated privileges. Exploitation requires existing local access and depends on the Agent's inventory collection processing the crafted path.	7.8	More Deta
CVE-2026-119578	MONAI from 1.6.0 before 1.6.1 contains a remote code execution vulnerability in Auto3DSeg algo_from_json() that allows attackers to run Python code via a crafted work directory's algo_object.json. Attackers can ship a malicious algorithm_templates module plus a _target_ name that is imported and instantiated when victims call AutoRunner or import_bundle_algo_history, executing code under default configuration.	7.8	More Deta
CVE-2026-119116	A use-after-free and double-free issue in the SetClient command handler of the kmstool-enclave sample application of AWS aws-nitro-enclaves-sdk-c before 0.4.6 may allow an application that runs on the parent EC2 instance to corrupt heap memory inside a Nitro Enclave which may lead to arbitrary code execution within the enclave. To remediate this issue, users should rebuild any enclave image that includes kmstool-enclave, or code derived from it, against aws-nitro-enclaves-sdk-c 0.4.6.	7.8	More Deta
CVE-2026-101213	Dell OpenManage Enterprise, versions prior to 4.8.0, contains an Improper Privilege Management vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges.	7.8	More Deta
CVE-2026-119722	Blender before 4.5.15 and 5.x before 5.2.3 contains a heap out-of-bounds access vulnerability in read_struct() that skips size validation when a .blend file's SDNA struct layout compares equal. Attackers can supply a crafted .blend file with short blocks so field reads, writes, and pointer dereferences overrun heap memory, causing crashes or code execution.	7.8	More Deta
CVE-2026-119718	Blender before 4.5.15 and 5.x before 5.2.3 contains a heap buffer overflow vulnerability caused by integer overflow in ptcache_data_alloc() when reading point cache files. Attackers can supply a crafted point cache file with a large totpoint value alongside a .blend file to crash Blender or execute code as the user.	7.8	More Deta
CVE-2026-104062	Scribus before 1.6.7 and 1.7.x before 1.7.4 contains a heap buffer overflow vulnerability in the PICT image loader and import plugin that allows attackers to corrupt heap memory by supplying an unchecked bytesPerLine value. Attackers can craft a PICT file whose bytesPerLine exceeds the QImage scanline size, so placing or importing it crashes Scribus and may execute code as the user.	7.8	More Deta
CVE-2026-104064	Scribus before 1.6.7 and 1.7.x before 1.7.4 contains an integer overflow vulnerability in the scimgdataloader_tiff TIFF loader that allows attackers to trigger a heap overflow via crafted tile dimensions. Attackers can supply a tiled TIFF with large tile width, height and sample values for a user to import, corrupting heap memory to crash Scribus or execute code.	7.8	More Deta
CVE-2026-104065	Scribus before 1.6.7 and 1.7.x before 1.7.4 contains an out-of-bounds write vulnerability in the importdrw Micrografx Draw plugin that uses an unvalidated y offset to select image scanlines. Attackers can craft a DRW file that, when imported by a user, writes decoded bitmap data outside the heap image buffer, causing crashes or code execution.	7.8	More Deta
CVE-2026-119250	A malicious actor with local access and low privileges could exploit an External Control of File Name or Path vulnerability found in WiFiman Desktop to execute arbitrary commands with root privileges on the host device.	7.8	More Deta
CVE-2026-119373	SQLite before 3.54.0 built with FTS5 contains a heap buffer overflow in fts5MergeRowidLists() that undersizes the output buffer when merging detail=none prefix doclists. Attackers who can populate a detail=none FTS5 table with negative rowids and run a prefix MATCH query can write past the allocation, corrupting heap memory and crashing the process.	7.8	More Deta
CVE-2026-119586	SQLite command-line shell through 3.54.1 contains a command injection vulnerability in the .recover command that emits attacker-planted dot-commands stored in sqlite_schema.sql values verbatim. Attackers can craft a database whose schema holds a valid CREATE statement followed by a .shell or .system line, executing OS commands when victims pipe .recover output into sqlite3.	7.8	More Deta
CVE-2026-118378	Tabularis before 0.28.0 contains an SQL injection vulnerability in its SQLite driver that allows MCP clients to execute stacked statements by supplying a crafted table_name to the describe_table tool. Attackers, including AI agents steered by untrusted content, can close the quoted PRAGMA argument and append statements to read, modify, or drop SQLite data, bypassing read-only mode and write approval.	7.8	More Deta
CVE-2026-51831	An issue in IDrive IDrive Backup for Windows Version 7.0.1.1 and below affected, remediated in Version 7.0.1.2 allows a local attacker to execute arbitrary code via the id_service.exe component	7.8	More Deta

CVE-2026-114148	Incorrect default permissions in ASP.NET Core allows an authorized attacker to elevate privileges locally.	7.8	More Deta
CVE-2026-51832	An issue in IDrive IDrive Backup for Windows Version 7.0.1.1 and below affected, remediated in Version 7.0.1.2 allows a local attacker to execute arbitrary code via the id_service.exe component	7.8	More Deta
CVE-2026-78402	Stack-based buffer overflow and out-of-bounds write vulnerability in Thales Sentinel Keys Server on Windows allows Overflow Buffers. Sentinel Keys Server does not check the length of the first field in the input message. A local attacker may craft an input and send it to Sentinel Keys Server. It may lead to code execution as NT AUTHORITY\SYSTEM enabling local privilege escalation. This issue affects Sentinel Keys Server: versions lower than 1.3.8.0.	7.8	More Deta
CVE-2026-119336	Pi-hole is a DNS sinkhole that protects devices from unwanted content without installing any client-side software. From 6.4.2 until 6.5, the root-run advanced/Scripts/updatecheck.sh cron job applies truncate -s 0 and chmod 644 to /etc/pihole/versions while following symbolic links in a directory owned by the pihole user. An attacker executing as pihole can replace that path with a symlink so the scheduled root operations truncate or create an arbitrary root-owned file, or race the operations so chmod makes a sensitive target world-readable without truncating it. This issue is fixed in version 6.5.	7.8	More Deta
CVE-2026-119335	Pi-hole is a DNS sinkhole that protects devices from unwanted content without installing any client-side software. Prior to 6.5, advanced/Scripts/utils.sh getFTLPID() attempts to validate the pihole-owned /run/pihole-FTL.pid file with expr "${FTL_PID}" : "[^[:digit:]]", but this rejects only values whose first character is not a digit. An attacker with code execution as the pihole user can write a digit-prefixed arithmetic expression to the pihole-owned PID file. Root-run pihole subcommands then evaluate [["$pid" -eq "-1"]], causing Bash to recursively evaluate array subscripts and execute command substitution as root. This bypasses the content-validation portion of the CVE-2026-41489 remediation while leaving its hardcoded PID-file path protection intact. This issue is fixed in version 6.5.	7.8	More Deta
CVE-2026-119333	draw.io Desktop is the official Electron build of draw.io. Prior to 31.5.2, the Windows application launched powershell and attrib by bare executable name from src/main/electron.js. When draw.io Desktop was not already running, opening a diagram from File Explorer made the diagram directory the current working directory, allowing a colocated attacker-controlled powershell.bat or attrib.exe to be resolved before the intended system executable. A victim who extracted an attacker-supplied archive and cold-opened its legitimate .drawio file could therefore execute attacker-controlled code when Local Fonts were enabled or when draft or backup attributes were updated. This issue is fixed in version 31.5.2.	7.8	More Deta
CVE-2026-104066	Scribus before 1.6.7 and 1.7.x before 1.7.4 contains a heap buffer overflow vulnerability in the Mac PICT image loader and import plugin when unpacking 4-bit indexed pixel data. Attackers can supply a crafted PICT file with inconsistent width and row data that, when placed or imported, writes out of bounds, causing crashes or code execution.	7.8	More Deta
CVE-2026-99116	In the Linux kernel, the following vulnerability has been resolved: net: psp: do not inherit the Rx association on clone sk->psp_assoc sits past sk_dontcopy_end, so sock_copy() copies it into every socket accepted from a listener without taking a reference, while inet_sock_destruct() puts for every inet socket. psp_twsk_init() does refcount_inc() for the timewait socket, so a child closing through TIME_WAIT cancels its own put and leaves the association with one reference and N timewait sockets holding the same pointer. Closing the listener frees it, and the timewait timers then put freed memory. Rejecting the association on a listening socket is not sufficient: a socket can acquire one while established and then be turned back into a listener, because tcp_disconnect() leaves sk->psp_assoc in place. BUG: KASAN: slab-use-after-free in psp_twsk_assoc_free+0x6f/0xf0 Write of size 4 at addr ffff888110f9255c by task swapper/7/0 psp_twsk_assoc_free+0x6f/0xf0 inet_twsk_put+0xda/0x1b0 call_timer_fn+0x53/0x2e0 __run_timers+0x764/0xa80 Freed by task 99: kfree+0x1a7/0x500 process_one_work+0x7ec/0x1100 An association carries a per-connection SPI and key, so a child must not inherit the parent's. Clear it on clone.	7.8	More Deta
CVE-2026-84294	Improper limitation of pathname in the Ad Hoc Transfer component of Progress Software WS_FTP Server versions prior to 2024.0.6 and 2025.0.3 on Windows could allow an authenticated user to access files outside intended directories.	7.7	More Deta
CVE-2026-100105	A user with permission to edit contact points but not their protected fields can change protected settings, such as a contact point's destination URL, by switching an integration to a legacy schema version, which can expose stored credentials and redirect alert notifications (incorrect authorization).	7.7	More Deta
CVE-2026-88967	A user with query access to an Azure Monitor data source in Grafana can cause server-side requests to an attacker-controlled endpoint that disclose the data source's Azure access token (server-side request forgery).	7.7	More Deta
CVE-2026-118644	n8n before 2.41.5 and 2.42.x before 2.42.2 passes a failed workflow's full execution context, including the identity of the user who started the run, to the configured error workflow. A project editor can set a colleague's workflow settings.errorWorkflow to an error workflow they own, inherit the colleague's identity when that workflow fails, and resolve the colleague's per-user dynamic credential secrets.	7.7	More Deta
CVE-2026-13451	A flaw was found in KServe. A namespace-scoped user with create/update permissions on InferenceService custom resources can exploit this vulnerability by providing a malicious `storageUri`. This Server-Side Request Forgery (SSRF) vulnerability allows the `storage-initializer` init container to issue arbitrary outbound HTTP/HTTPS requests from inside the cluster. This can lead to information disclosure, including credential theft for the node's Identity and Access Management (IAM) role or access to internal cluster services.	7.7	More Deta
CVE-2026-54455	OpenCATS is an open-source applicant tracking system and recruitment CRM for staffing agencies and hiring teams. Prior to version 0.10.0, activity DataGrid date filtering in `home:CallsDataGrid` and `activity:ActivityDataGrid` uses request-controlled `period`, `startDate` and `endDate` parameters without sufficient validation or escaping. The vulnerable code is in `modules/home/dataGrids.php` and `modules/activity/dataGrids.php`. The `startDate` and `endDate` values are inserted into SQL string comparisons without safe escaping, and `period` can directly influence generated SQL. An authenticated user with access to the affected DataGrid endpoints can alter the intended query to access sensitive database contents, including user account data, candidate records, contact details, company information, job orders and activity history. A valid OpenCATS login is required; unauthenticated exploitation is not established. This issue is fixed in version 0.10.0.	7.6	More Deta
CVE-2026-86377	Dell PowerProtect Data Domain, Feature Release versions 7.7.1.0 through 8.8, LTS2024 release versions 7.13.1.0 through 7.13.1.80, LTS2025 release versions 8.3.1.0 through 8.3.1.40, LTS2026 release versions 8.6.1.0 through 8.6.1.20, contain an Out-of-bounds Write vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Denial of service.	7.6	More Deta
CVE-2026-112347	Kirki plugin for WordPress before 6.4.1 contains a broken object-level access control vulnerability in its page REST API, where the PUT /wp-json/kirki/v1/pages/{page_id} route and the save_page_data, duplicate, and delete handlers in PageController.php rely only on a coarse role-to-access middleware check without performing a per-object WordPress capability check. A user with Kirki edit access, granted to the Editor role by default, can exploit this flaw to modify the title, slug, and publication status of any non-trashed post of any post type, including custom post types and WooCommerce products they do not own, exposing private or draft content or removing published content by manipulating the unrestricted post_status field.	7.6	More Deta
CVE-	FreeMail before 5.3.2 contains an authorization bypass vulnerability that allows authenticated users to claim another user's existing mailbox via		More

2026-119049	the POST /api/create endpoint. Attackers who know a victim's address can become co-owners through assignMailboxToUser to read messages and verification codes, set forwarding, and delete mail.	7.6	Deta
CVE-2026-45145	Chamilo LMS is an open-source learning management system. Prior to 2.0.1, `public/main/inc/lib/career.lib.php` and `public/main/cron/import_csv.php` call PHP's native `unserialize()` on `user_career.extra_data` retrieved from the database without the `allowed_classes: false` safety option. An attacker able to write crafted serialized PHP objects to that column, for example through a separate SQL injection, a compromised admin CSV import, or a lower-privilege admin panel, can instantiate arbitrary PHP objects and trigger POP gadget chains in autoloaded `Symfony`, `Doctrine`, or `Monolog` components. This permits arbitrary OS commands as the web server user, compromising server confidentiality, integrity, and availability. This issue is fixed in version 2.0.1.	7.5	More Deta
CVE-2026-61739	SOCFortress CoPilot focuses on providing a single pane of glass for all your security operations needs. Prior to 0.1.77, the Velociraptor Sigma exclusion-management endpoints in `backend/app/incidents/routes/incident_alert.py` omit role and tenant authorization, and `POST /api/incidents/alerts/create/velo-sigma/exclusion` does not validate credentials. Its `return_username_for_logging` dependency in `backend/app/auth/utils.py` calls `decode_token`, which returns ordinary Invalid token or Expired signature strings on failure, and the dependency passes these strings through instead of rejecting the request. A Bearer header is required, but an arbitrary invalid, expired or forged value can create a suppression rule without a valid account. The collection GET at /create/velo-sigma/exclusion lists exclusions; the read, update and delete routes under `/create/velo-sigma/exclusion/{exclusion_id}`, and the `/velo-sigma/exclusion/{exclusion_id}/toggle` route, use `get_current_user` without role checks, permitting any authenticated `customer_user` to manage every exclusion. In `backend/app/incidents/services/velo_sigma.py`, `process_sigma_alert` calls `check_exclusions` and drops matching enabled alerts before incident creation. A null `customer_code` applies a rule across all tenants. Attackers can suppress detections platform-wide through channel, title or field matching, while low-privilege accounts can enumerate detection-tuning data and modify, disable or delete legitimate exclusions. This issue is fixed in version 0.1.77.	7.5	More Deta
CVE-2026-103410	An Integer Overflow vulnerability in the DPI certificate scanner in Juniper Networks Session Smart Router allows an unauthenticated remote attacker to cause a denial of service via a specially crafted TLS server certificate.	7.5	More Deta
CVE-2026-114443	The Security Plugin, Firewall & Malware Scanner with Auto Removal WordPress plugin before 2.191 does not verify the account password before accepting an authenticator-app two-factor code at login, allowing anyone who holds a user's current authenticator code to log in as that user, including an administrator, without the password.	7.5	More Deta
CVE-2026-119656	CoreShop by CoreUnion through 1.5.5 contains an unauthenticated sql injection vulnerability in the api/Agent/GetGoodsPageList endpoint via the order parameter appended to an ORDER BY clause. Anonymous attackers can inject subqueries that bypass SqlSugar's field check to extract member accounts and orders through boolean-based or time-based blind techniques.	7.5	More Deta
CVE-2026-110732	The AI Engine – The Chatbot, AI Framework & MCP for WordPress plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 3.8.6 This is due to the MCP module's OAuth 2.1 Dynamic Client Registration endpoint (/wp-json/mcp/v1/oauth/register) being registered with a permission_callback of __return_true, allowing an unauthenticated user to register an active OAuth client with an attacker-controlled redirect URI. This makes it possible for unauthenticated attackers to obtain an administrator-bound MCP access token, and thereby full administrator-level control through the MCP tools (including user creation and option updates), once an administrator approves the attacker's client on the OAuth consent screen. The consent page is additionally served without X-Frame-Options or Content-Security-Policy frame-ancestors, so that approval can be obtained via clickjacking.	7.5	More Deta
CVE-2026-119426	phpMyAdmin through 5.2.3 contains a cross-site request forgery vulnerability that allows remote attackers to execute arbitrary SQL by bypassing CSRF token checks on non-AJAX POST requests. Attackers can lure authenticated victims into submitting cross-site POSTs carrying sql_query to /sql or /database/sql, running SQL with the victim's database privileges under http or config authentication.	7.5	More Deta
CVE-2010-20125	DedeCMS before 5.7 contains a file inclusion vulnerability in plus/carbuyaction.php that allows remote unauthenticated attackers to control the include path by manipulating the uninitialized code parameter passed to require_once. Attackers can supply path traversal sequences ../../ to include arbitrary local files outside the intended payment directory, potentially achieving local file disclosure. Exploitation evidence was first observed by the Shadowserver Foundation on 2023-10-18.	7.5	More Deta
CVE-2026-114422	The Enable Media Replace WordPress plugin before 4.2.3 does not restrict the classes allowed when deserializing stored metadata during its media replace-and-update-links routine, allowing unauthenticated users to inject a PHP object that is instantiated when a user with upload access performs a routine media replacement, resulting in PHP Object Injection and local file inclusion of existing PHP/HTML files, which can be escalated to remote code execution where an attacker-influenced PHP or HTML file is present on the server. This is a regression of CVE-2023-4643, which was fixed in 4.1.3 and reintroduced in 4.1.4.	7.5	More Deta
CVE-2026-119655	CoreShop through 1.5.5 contains an unauthenticated sql injection vulnerability in the api/Good/GetGoodsPageList endpoint via the unvalidated order parameter appended to ORDER BY. Attackers can inject subqueries that bypass SqlSugar's field check and use boolean-based or time-based blind techniques to extract member accounts and orders.	7.5	More Deta
CVE-2026-110245	IBM Langflow OSS 1.0.0 through 1.12.4 could allow a remote attacker to obtain sensitive information due to improper authentication.	7.5	More Deta
CVE-2026-117183	A path traversal vulnerability in the FeaturedImage component of astro-notion-blog 0.13.0 allows attackers to escape the intended directory, as well as read and overwrite files on the server via a crafted URL.	7.5	More Deta
CVE-2026-76012	The Photo Gallery, Sliders, Proofing and Themes – NextGEN Gallery plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 4.4.1 via the legacy_render function. This is due to broken authorization on the Lightroom gallery_edit endpoint combined with mass assignment of gallery path and unrestricted file upload into a registered template directory, whose extension check uses a substring match that accepts sanitized .php_ filenames as valid templates. This makes it possible for authenticated attackers, with custom-level access and above, to execute code on the server. Exploitation requires the authenticated attacker to be the stored author of at least one existing NextGEN gallery, as ownership of that gallery is the sole authorization check gating the mass-assignment and upload steps.	7.5	More Deta
CVE-2026-111578	The PDF Invoices & Packing Slips for WooCommerce WordPress plugin from 5.16.2 before 5.16.5 does not properly escape several customer-supplied order fields — including the billing and shipping address values and the customer order note — before they are output in generated invoice and packing-slip documents, allowing unauthenticated users placing guest orders to store a malicious script that executes when a shop administrator views the document, leading to Stored Cross-Site Scripting.	7.5	More Deta
CVE-2026-	ESPAsyncWebServer is an asynchronous HTTP and WebSocket server library for ESP32, ESP8266, RP2040 and RP2350. Prior to version 3.11.2, the multipart parser in `src/WebRequest.cpp` frees `_itemBuffer` and sets it to NULL when `BOUNDARY_OR_DATA` matches the closing boundary of a file part, before confirming the following terminator, while leaving `_itemIsFile` true. If the next byte is neither the final closing dashes nor a clean CRLF, the `DASH3_OR_RETURN2` or `EXPECT_FEED2` rewind branch re-injects provisionally consumed bytes through `itemWriteByte`. Because	7.5	More Deta

62966	`_itemIsFile` remains true, `_itemBuffer`[`_itemBufferIndex`++] writes through a null pointer. On ESP32 this causes a `StoreProhibited` exception, panic and device reboot, producing remote denial of service. A route with a non-trivial body/upload handler, such as a file-upload or web-OTA endpoint, must be present. This issue is fixed in version 3.11.2.		
CVE-2026-62864	Ring is a Clojure web applications library inspired by Python's WSGI and Ruby's Rack. Prior to 1.15.5, `wrap-nested-params` in the `ring.middleware.nested-params` namespace uses a backtracking regular expression to match parameter names from URL query strings and HTTP request bodies. An attacker can craft a parameter name that drives quadratic O(n^2) matching work, causing regular-expression denial of service in applications using the middleware. `Ring-Defaults` users are also exposed because nested-params is enabled by default. Applications omitting the middleware do not expose this parsing path. This issue is fixed in version 1.15.5.	7.5	More Deta
CVE-2026-62297	ag-psd is a JavaScript library for reading and writing Photoshop Document files. Before the allocation-limit remediation attempt in version 31.0.0, `readPsd()` commits image and layer buffers from attacker-declared PSD geometry before validating the declarations against the actual available data or sane allocation limits. The `psdReader.js` implementation sizes off-heap typed arrays using `width`, `height`, `channels`, `depth` and `per-layer rectangles`, so a tiny PSD declaring enormous geometry can force multi-gigabyte memory allocation before a later bounds error. The reported 52-byte input on Node 24 produced approximately 3.17 GB peak RSS before a RangeError; under memory pressure the process can be terminated before the error can be caught, and concurrent inputs can exhaust memory. Services reading untrusted PSDs are exposed to denial of service. This differs from genuinely large PSD files whose memory demand is proportional to real input content. Version 31.0.0 adds a composite-image allocation limit, but complete coverage of the separately described layer-rectangle allocation path is not established and requires curator residual/scope review.	7.5	More Deta
CVE-2026-99152	In the Linux kernel, the following vulnerability has been resolved: scsi: libiscsi: Validate the task named by a management response __iscsi_complete_pdu() fetches the task for five response types from one place and checks only that the index resolved: case ISCSI_OP_LOGOUT_RSP: case ISCSI_OP_LOGIN_RSP: case ISCSI_OP_TEXT_RSP: case ISCSI_OP_SCSI_TMFUNC_RSP: case ISCSI_OP_NOOP_IN: task = iscsi_itt_to_task(conn, hdr->itt); if (!task) return ISCSI_ERR_BAD_ITT; iscsi_itt_to_task() bounds the index against cmds_max and looks at nothing else, so a target can name any slot in the pool, including one that has never been used. task->conn is then NULL, and both iscsi_nop_out_rsp() and iscsi_complete_task() dereference it. One unsolicited NOP-In is enough; a Text Response carrying the same ITT crashes in iscsi_complete_task() instead. Require the task to be in flight and not a SCSI command, the way iscsi_itt_to_ctask() does for the command opcodes. [6.298634] Oops: general protection fault, probably for non-canonical address 0xdffffc000000000c: 0000 [#1] SMP KASAN NOPTI [6.298642] KASAN: null-ptr-deref in range [0x0000000000000060-0x0000000000000067] [6.298652] CPU: 1 UID: 0 PID: 111 Comm: iscsistart Not tainted 7.2.0-rc5-ISCSI1-gf5098b6bae76 #1 PREEMPT(lazy) [6.298654] Hardware name: QEMU Ubuntu 24.04 PC v2 (i440FX + PIIX, arch_caps fix, 1996), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 [6.298656] RIP: 0010:iscsi_nop_out_rsp.constprop.0+0x46/0x160 [6.298691] Code: c1 ea 03 48 83 ec 08 80 3c 02 00 0f 85 f5 00 00 00 48 b8 00 00 00 00 00 fc ff df 48 8b 6b 58 48 8d 7d 60 48 89 fa 48 c1 ea 03 <80> 3c 02 00 0f 85 c0 00 00 00 48 8b 45 60 48 39 c3 74 50 48 b8 00 [6.298698] RSP: 0018:ffff88806c907be8 EFLAGS: 00010206 [6.298701] RAX: dfffc0000000000 RBX: ffff888006116800 RCX: 0000000000000020 [6.298702] RDX: 000000000000000c RSI: ffff88800525d578 RDI: 0000000000000060 [6.298703] RBP: 0000000000000000 R08: 0000000000000000 R09: 0000000000000000 [6.298706] R10: 0000000000000020 R11: 0000000000000000 R12: 0000000000000000 [6.298706] R13: 000000000000002e R14: ffff8880056eb440 R15: ffff888006116800 [6.298707] FS: 00007fc02d1c2740(0000) GS:ffff8880b29bc000(0000) knlGS:0000000000000000 [6.298710] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [6.298711] CR2: 000055fe3b56ddf8 CR3: 00000000053b9004 CR4: 0000000000770ef0 [6.298712] PKRU: 55555554 [6.298713] Call Trace: [6.298714] <IRQ> [6.298714] __iscsi_complete_pdu+0x13a8/0x22a0 [6.298758] iscsi_complete_pdu+0x54/0xa0 [6.298759] iscsi_tcp_hdr_recv_done+0x870/0x2c80 [6.298778] iscsi_tcp_recv_skb+0x31e/0xec0 [6.298800] iscsi_sw_tcp_recv+0x12f/0x390 [6.298804] __tcp_read_sock+0x1ab/0x810 [6.298812] iscsi_sw_tcp_data_ready+0x18b/0x510 [6.298814] tcp_rcv_established+0x1f56/0x3a00 [6.298842] tcp_v4_do_rcv+0x449/0x960 [6.298847] tcp_v4_rcv+0x2245/0x3bc0	7.5	More Deta
CVE-2026-116243	pgAdmin 4 runs pg_dump, pg_restore, pg_dumpall and psql from the binary path a user sets in their preferences. In server mode the binary path was refused only when it lay under the per-user storage directory (STORAGE_DIR), not under a SHARED_STORAGE directory, which ordinary users can upload files to. A user could therefore upload an executable to shared storage, point their binary path at it, and have pgAdmin run it as the operating-system account running pgAdmin. On POSIX, files created through pgAdmin are not executable, so this is exploitable where any file with an executable name can run, such as Windows server mode. The fix checks the binary path against every SHARED_STORAGE directory as well, after expanding $DIR, collapsing ".." and resolving symbolic links, compares directories in a way a different spelling on a case-insensitive filesystem cannot bypass, refuses a path containing a NUL, and enforces the check wherever binary paths are resolved, including for the PSQL tool. This issue affects pgAdmin 4: before 9.19.	7.5	More Deta
CVE-2026-62264	PDF Reader MCP is a Model Context Protocol server for reading PDF documents. In versions 2.2.0 and later prior to 3.0.1, when `MCP_TRANSPORT=http` enables the opt-in HTTP server, `@sylphx/pdf-reader-mcp` reads `MCP_API_KEY` and logs that `X-API-Key` authentication is enabled but never validates the `X-API-Key` header on incoming requests. The `/mcp` endpoint consequently accepts unauthenticated clients. With the default bind address of `0.0.0.0`, any client able to reach the port can invoke every PDF tool and read any PDF the server process can open on the host, despite the misleading authentication-enabled startup log. URL-based sources additionally permit limited server-side request forgery; private and loopback destinations are blocked by default unless `--allow-private-ips` is set. The default `stdio` transport is unaffected. This issue is fixed in version 3.0.1.	7.5	More Deta
CVE-2026-59978	AdminNeo is a full-featured database management tool written in PHP. From 4.6.2 until 5.5.0, the unauthenticated `?script=version` endpoint accepts POST data without origin, CSRF or parameter-type validation. A `version[]` parameter becomes a PHP array that `bootstrap.inc.php` serializes into the shared `adminneo.version` cache. On later page loads, `design.inc.php` passes that cached value to `cookie()` and `rawurlencode()`, causing a `TypeError` rather than encoding a version string. A remote attacker can make the instance return HTTP 500 to all users for the cache's twenty-four-hour lifetime or until the poisoned cache is removed. Exploitation requires the web server to be able to write that shared cache; making it unwritable is an interim workaround. The issue retains the underlying type-validation defect reported previously in Adminer despite changes to AdminNeo's version-checking flow. This issue is fixed in version 5.5.0.	7.5	More Deta
CVE-2026-46560	Open Access Management (OpenAM) is an access management solution. Prior to 16.1.1, the `RADIUS` authentication module opens an unconnected datagram socket and trusts the first UDP datagram received on the client source port. The receive path does not verify the source IP and port, match the response identifier to the outstanding request, or verify the RFC 2865 `Response Authenticator`; the RFC 2869 `Message-Authenticator` is neither sent nor required. Any non-Reject/non-Challenge packet is treated as success. On a deployment with a `RADIUS` module instance enabled on a login chain, an unauthenticated network attacker can race the real server on-path or spray forged `Access-Accept` packets off-path and obtain a session for any `RADIUS`-mapped username without knowing the shared secret. Unlike CVE-2024-3596, exploitation requires no MD5 chosen-prefix forgery because no response authenticator is checked. The resulting session carries the impersonated principal's privileges. This issue is fixed in version 16.1.1.	7.5	More Deta
CVE-2026-39734	Unauthenticated Path Traversal in WP EasyPay <= 4.5.4 versions.	7.5	More Deta
CVE-2026-116862	Unauthenticated Broken Access Control in WP REST Cache <= 2026.3.1 versions.	7.5	More Deta
CVE-			

2026-116861	Unauthenticated Sensitive Data Exposure in Flexible Chat <= 1.1.0 versions.	7.5	More Deta
CVE-2026-116401	Unauthenticated Broken Access Control in HUSKY <= 1.4.6 versions.	7.5	More Deta
CVE-2026-97638	The Forminator Forms – Contact Form, Payment Form & Custom Form Builder plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 1.57.3.1 via the 'previous_draft_id' parameter due to missing validation on a user controlled key. This makes it possible for unauthenticated attackers to delete arbitrary saved drafts belonging to other users and take over those draft identifiers by overwriting them with attacker-controlled form submissions. This requires the attacker to have obtained a victim's draft_id, which may be harvested from a shared "continue later" link; the nominally present nonce check is effectively bypassed because the nonce is publicly obtainable by any unauthenticated visitor loading a form page.	7.5	More Deta
CVE-2026-115591	Insertion of Sensitive Information Into Sent Data vulnerability in Supsystic Contact Form by Supsystic contact-form-by-supsystic allows Retrieve Embedded Sensitive Data.This issue affects Contact Form by Supsystic: from n/a through 1.10.5.	7.5	More Deta
CVE-2026-117184	An issue in the GraphQL endpoint of traggo server v0.8.3 allows attackers to cause a Denial of Service (DoS) via a crafted POST request to the GraphQL endpoint	7.5	More Deta
CVE-2026-119762	Axigen Mail Server before 10.5.69, 10.6.x before 10.6.40, and 10.7.x before 10.7.2 contains an unauthenticated denial of service vulnerability caused by unbounded nesting depth when parsing SOAP/XML and JSON request bodies before authentication. Attackers can send a single deeply nested request to WebMail, WebAdmin, or WebMail Proxy listeners to exhaust the stack and crash SMTP, IMAP, POP3, and web services repeatedly.	7.5	More Deta
CVE-2026-116393	Missing Authorization vulnerability in iHomefinder, Inc. Optima Express optima-express allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Optima Express: from n/a through 9.0.0.	7.5	More Deta
CVE-2026-118035	In Progress® Telerik® Document Processing Libraries prior to version 2026.3.1027, uncontrolled recursion, inefficient algorithmic complexity and infinite loop vulnerabilities in RadWordsProcessing allow an unauthenticated attacker to terminate or hang the host process via a crafted DOCX, DOC, RTF or HTML document.	7.5	More Deta
CVE-2026-118036	In Progress® Telerik® Document Processing Libraries prior to version 2026.3.1027, uncontrolled recursion, infinite loop, inefficient algorithmic complexity and resource allocation vulnerabilities in RadPdfProcessing and AI document summarization and question answering allow an unauthenticated attacker to terminate or hang the host process via a crafted PDF document or document text submitted for summarization or question answering.	7.5	More Deta
CVE-2026-118037	In Progress® Telerik® Document Processing Libraries prior to version 2026.3.1027, uncontrolled recursion, infinite loop, unchecked loop condition and inefficient regular expression vulnerabilities in RadSpreadProcessing and RadSpreadStreamProcessing allow an unauthenticated attacker to terminate or hang the host process via a crafted XLSX or XLS workbook or formula.	7.5	More Deta
CVE-2026-118039	In Progress® Telerik® Document Processing Libraries prior to version 2026.3.1027, an XML external entity reference vulnerability in SVG image processing allows an unauthenticated attacker to read local files on the server via a crafted SVG image with a nested embedded SVG, when the image is processed or exported to PDF.	7.5	More Deta
CVE-2026-118040	In Progress® Telerik® Document Processing Libraries prior to version 2026.3.1027, improper verification of cryptographic signatures and improper certificate validation in RadPdfProcessing digital signature validation allow an unauthenticated attacker to cause signature validation to report forged content as unmodified and its signing certificate as valid via a crafted signed PDF document.	7.5	More Deta
CVE-2026-119760	sniproxy through 0.7.0 contains a NULL pointer dereference vulnerability in resolv_cancel() that allows remote unauthenticated attackers to crash the daemon by sending overlong hostnames. Attackers can send a 254 or 255 character TLS SNI name or HTTP Host header matching a wildcard backend, then close the connection to terminate the proxy.	7.5	More Deta
CVE-2026-110305	The Advanced Custom Fields: Extended plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 0.9.2.7 via the process. This makes it possible for unauthenticated attackers to extract sensitive data including the WordPress password hash of any user by injecting a {get_user} template tag that is resolved and written as a publicly readable term name. Exploitation requires that an administrator has configured a public [acfe_form] shortcode page with a Term action using a save.name field mapping — a supported and documented configuration.	7.5	More Deta
CVE-2026-107630	The Email Templates Customizer and Designer for WordPress and WooCommerce plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.5.14 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 enumerate WooCommerce order IDs via the preview_order parameter and exfiltrate every customer's billing name, address, phone number, and email address. The exploit requires two unauthenticated requests: the first harvests a reusable nonce from the 302 Location header returned by the unguarded admin_init handler, and the second supplies that nonce alongside an arbitrary order ID to the preview endpoint, making full customer PII disclosure trivially achievable without any account or credentials.	7.5	More Deta
CVE-2026-116795	RE2JS is the JavaScript port of RE2, a regular expression engine that provides linear time matching. From 2.2.0 until 2.8.7, enabling LOOKBEHINDS and using repeated matching through matcher().find(), matchAll(), split(), or matcher().replaceAll() can cause quadratic total work. Machine.match restarts lookbehind scanning from offset zero for each requested start position, while Matcher-based APIs request capture slots that prevent the early exit used for captureless matching. Dense matches therefore repeatedly rescan the input, allowing attacker-influenced text to monopolize a single-threaded worker and deny service. This issue is fixed in version 2.8.7.	7.5	More Deta
CVE-2026-119290	Zuke is a code-first, strongly typed build automation system for Deno. Prior to 1.51.0, @zuke/core writes rendered reportSummary(...) notes to GITHUB_STEP_SUMMARY through writeJobSummary without applying the redactor that protects resolved secret() values in console and persisted run output. A GitHub Actions build that places secret-derived text in a summary note can publish credentials in cleartext to everyone able to view the workflow run, including unauthenticated viewers of a public repository, and the durable summary remains exposed until the run is deleted. GitHub Actions masking directives do not protect the summary file, while runs outside GitHub Actions and builds that do not summarize secret-derived text are not affected. This issue is fixed in version 1.51.0.	7.5	More Deta
CVE-2026-106971	An integer overflow in the MessagePack\BufferUnpacker component of rybakit/msgpack versions prior to 0.11.0 allows attackers to cause a denial of service via crafted MessagePack input when the application runs on 32-bit PHP	7.5	More Deta
CVE-	Uncontrolled recursion in MessagePack\BufferUnpacker::unpack() in rybakit/msgpack versions prior to 0.11.0 allows attackers to cause a denial of		More

2026-106972	service through memory exhaustion when an application decodes deeply nested, attacker-controlled MessagePack input.	7.5	Deta
CVE-2026-103963	A flaw was found in glib-networking. When establishing connections using Transport Layer Security (TLS) version 1.3, the client-side session cache does not limit the number of session tickets retained for a single host. A malicious server can exploit this by sending excessive session ticket messages, causing the client application to continuously consume memory. This unbounded memory growth can exhaust system memory, resulting in a Denial of Service (DoS).	7.5	More Deta
CVE-2026-119202	@hapi/content provides HTTP Content-* header parsing. From 3.0.6 until 6.0.3, Content.disposition() uses an unanchored parameter-name expression in a global regular-expression scan, causing repeated failed matching over the remaining input when a Content-Disposition parameter contains a long token without an equals sign. The resulting quadratic processing can block the Node.js event loop before route handlers or validation when @hapi/pez parses multipart/form-data headers, including unauthenticated hapi routes with payload.multipart enabled, and also affects applications that pass untrusted headers directly to Content.disposition(). This issue is fixed in @hapi/content version 6.0.3.	7.5	More Deta
CVE-2026-119286	GraphQL-core is a Python port of the GraphQL.js reference implementation. From 3.3.0a3 until 3.3.1, validate() reuses a module-level ValidationAbortedError when a document exceeds max_errors. Python appends frames to the reused exception's traceback on every raise, retaining each document, validation context, and error set for the process lifetime. An unauthenticated client can repeatedly submit a small document with more than 100 validation errors to cause unbounded memory growth before query execution, eventually exhausting worker memory without disclosing or modifying data. This issue is fixed in version 3.3.1.	7.5	More Deta
CVE-2026-118758	Kubeflow Pipelines enables users to build and deploy portable, scalable machine learning workflows. Prior to 2.18.0, the volume artifact handler for GET /artifacts/get?source=volume did not confine a caller-supplied file path to the selected volume. A caller who can reach the route and identify an existing mounted volume can use path traversal to read files outside that volume when the artifact-serving process can read them. The frontend pod serves the request when artifact proxying is disabled, while the selected namespace's artifact-service pod serves it when proxying is enabled. A deployment with authentication disabled requires no application credentials; in multi-user deployments, the caller ordinarily must be authorized for the supplied namespace. This issue is fixed in version 2.18.0.	7.5	More Deta
CVE-2026-104895	The asynchronous Smile parser (NonBlockingByteArrayParser) uses a raw-binary length prefix taken from untrusted input to allocate a byte[] before the body is read, with no upper bound and no overflow check. On the raw-binary marker 0xFD, _decodeVInt() computes (value << 6) + (i & 0x3F) without the (value >>> 25) != 0 overflow guard present in the blocking SmileParser._readUnsignedVInt, and _startRawBinary then allocates the declared length immediately. A Smile feed of roughly ten bytes can therefore force an eager allocation of approximately 2 GB, producing an OutOfMemoryError on reactive or asynchronous Smile endpoints. A VInt crafted to overflow int yields a negative length and a NegativeArraySizeException, a RuntimeException that is not a JacksonException and so escapes the parser contract. Either outcome crashes the request or processing thread. This is the same class of issue as CVE-2020-28491 in the CBOR parser of this library, which was fixed with a LONGEST_NON_CHUNKED_BINARY guard; the asynchronous Smile parser never received the equivalent guard. No privileges or user interaction beyond the ability to submit data for parsing are required.	7.5	More Deta
CVE-2026-107052	Insecure permissions in the AIDL interface of ProjectMAXS MAXS Module FileRead versionCode 27 allows unauthorized attackers to arbitrarily reead files outside of the sandbox via providing an absolute path.	7.5	More Deta
CVE-2026-119052	llama.cpp b2877 before b11935 contains an uncaught exception vulnerability in the ggml-rpc server that allows unauthenticated remote attackers to crash the rpc-server by sending oversized message lengths. After the HELLO handshake, attackers can send a command such as SET_TENSOR with a length above std::vector::max_size(), triggering an uncaught std::length_error that aborts the process and denies service to all clients.	7.5	More Deta
CVE-2026-107055	Insecure permissions in the autosave component of AppML neutriNote CE versionCode 1387 allows unauthorized attackers to write arbitrary files.	7.5	More Deta
CVE-2026-107059	An issue in Nextcloud versionCode 30390190 allows attackers to force victim users to logout of their accounts and switch to an attacker controlled progile, bypassing authentication.	7.5	More Deta
CVE-2019-25781	Python-Markdown 3.0 through 3.11.2 contains an algorithmic complexity vulnerability in inline link parsing that allows remote attackers to exhaust CPU through unmatched brackets. Attackers can submit short Markdown containing repeated [or ![characters, forcing LinkInlineProcessor.getText() and getLink() into quadratic scans that keep workers busy for minutes.	7.5	More Deta
CVE-2026-119027	oapi-codegen 2.5.0 before 2.8.1 contains a code injection vulnerability that allows attackers to inject Go code by supplying a crafted servers[].x-go-name value emitted unescaped by the server-urls template. Attackers who control an OpenAPI document can define an injected func init() that executes when the victim builds and imports the generated package.	7.5	More Deta
CVE-2026-107049	An issue in Forkyz versionCode 8500000 allows attackers to arbitrarily change another user's storage settings via supplying a crafted URI string.	7.5	More Deta
CVE-2026-119025	open 7.2.0 before 11.0.0 contains an OS command injection vulnerability that allows attackers to execute PowerShell code by supplying crafted URLs on Windows and WSL. Attackers can embed $(...) subexpressions in URLs, such as OAuth authorization_endpoint values from malicious MCP servers, which execute when index.js passes them unescaped to powershell -EncodedCommand.	7.5	More Deta
CVE-2026-110184	The Newsmatic theme for WordPress is vulnerable to blind SQL Injection via the 'slug' parameter in all versions up to, and including, 1.5.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Deta
CVE-2026-118759	Kubeflow Pipelines enables users to build and deploy portable, scalable machine learning workflows. Prior to 2.18.0, the API server's GET /apis/v1alpha1/runs/{run_id}/nodes/{node_id}/log handler retrieved logs without authorizing the caller against the selected run. A caller who can reach the backend and knows a victim run ID and suitable pod or node identifier can read live or archived logs with the API server's permissions. For live logs, the caller-controlled node ID was also accepted as a pod name without verifying that the pod belonged to the requested run, allowing a known run ID to select the namespace of an unrelated pod and read its main container logs. The handler does not authenticate requests itself, although an external authentication gate or network policy can limit reachability. Exposed logs can contain sensitive workload data or credentials. This issue is fixed in version 2.18.0.	7.5	More Deta
CVE-2026-118761	Kubeflow Pipelines enables users to build and deploy portable, scalable machine learning workflows. Prior to 2.18.0, the API server decompressed uploaded pipeline archives without adequately bounding expanded data while locating or reading the pipeline file. A small ZIP or gzip-compressed tar archive can consume disproportionately large memory and exhaust API-server resources. Multipart pipeline and pipeline-version upload processing performs decompression before namespace authorization, so a reachable caller does not need a successful pipeline-create authorization decision. URL-import handlers authorize before fetching and decompressing a remote archive. The amount of expansion required to	7.5	More Deta

	interrupt service depends on deployment resource limits and concurrent activity, and no specific archive is guaranteed to crash every deployment. This issue is fixed in version 2.18.0.		
CVE-2026-115599	Missing Authorization vulnerability in ThimPress LearnPress learnpress allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects LearnPress: from n/a through 4.4.11.	7.5	More Deta
CVE-2026-114193	Missing Authorization vulnerability in Eyal Fitoussi GEO my WordPress geo-my-wp allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects GEO my WordPress: from n/a through 4.5.5.5.	7.5	More Deta
CVE-2026-107051	Insecure permissions in klassm AndFHEM v2.4.1 (versionCode 241, the verified build) allows unauthorized attackers to arbitrarily manipulate another user's FHEM home-automation control configurations.	7.5	More Deta
CVE-2026-107020	An issue in the activity.LoadLinkLaterActivity component of FeedEx / Handy News Reader versionCode 116 allows attackers to force victim users into fetching a crafted URL.	7.5	More Deta
CVE-2026-119283	joserfc is a Python library that provides an implementation of several JSON Object Signing and Encryption (JOSE) standards. Prior to 1.7.5, joserfc.jwe.decrypt_json() accepts a JWE General JSON Serialization recipients array without a count limit and calls decrypt_cek() for every entry. An unauthenticated attacker who can submit a JWE to an endpoint using an RSA key-management algorithm can choose the number of private-key decryption operations performed by one request. The verify_all_recipients option does not reduce this work because the affected loop processes every recipient before consulting that setting, allowing repeated requests to exhaust service CPU without affecting confidentiality or integrity. This issue is fixed in version 1.7.5.	7.5	More Deta
CVE-2026-107030	Insecure permissions in craftxbox YubiClip XOR fork v1.0.1 (versionCode 10003) allows unauthorized attackers to trigger the OTP-clipboard (One-Time Password) mechanism, causing a desynchronization of the timing.	7.5	More Deta
CVE-2026-118083	Unauthenticated Sensitive Data Exposure in WP Crowdfunding <= 2.2.2 versions.	7.5	More Deta
CVE-2026-119119	Crawl4AI before 0.9.5 contains a denial of service vulnerability in the Docker API server where _clamp_untrusted() fails to cap the delay_before_return_html, mean_delay, and max_range fields of untrusted CrawlerRunConfig bodies. Unauthenticated attackers can send huge values to /crawl or /crawl/stream to hold browser pages or stall the rate limiter, exhausting the page pool and blocking other crawls.	7.5	More Deta
CVE-2026-107042	Insecure permissions in USP Ultimate Screenshot Painter versionCode 240213.009 allows unauthorized attackers to move or overwrite files in another user's private storage via supplying a crafted content URI.	7.5	More Deta
CVE-2026-107041	Insecure permissions in the FeatureActionActivity component of Oasis Feng Island versionCode 51801 allows unauthorized attackers to arbitrarily force a freeze in the device, leading to a Denial of Service (DoS).	7.5	More Deta
CVE-2026-107039	Insecure permissions in the ActivityMain component of M66B/Marcel Bokhorst NetGuard no-root firewall versionCode 2026080101/versionName 2.337 allows unauthorized attackers to arbitrarily force a device reset or Denial of Service (DoS).	7.5	More Deta
CVE-2026-107037	Insecure permissions in the NotificationHelper component of NoNonsense Notes versionCode 72600 allows unauthorized attackers to write in another user's notes via supplying a note id.	7.5	More Deta
CVE-2026-107026	Insecure permissions in Share to Clipboard v1.14.1 (versionCode 32) allows unauthorized attackers to arbitrarily overwrite another user's clipboard content.	7.5	More Deta
CVE-2026-107024	Insecure permissions in Share 2 Archive Today versionCode 61 allows unauthorized attackers to arbitrarily overwrite another user's clipboard content via supplying a crafted URL.	7.5	More Deta
CVE-2026-107025	Insecure permissions in WikiAndPad alpha/beta v0.2alpha03 (versionCode 200300) allows unauthorized attackers to export the application's data.	7.5	More Deta
CVE-2026-119120	Crawl4AI from 0.9.0 before 0.9.5 fails to filter the CosineStrategy model_name field in untrusted Docker API request bodies, allowing authenticated clients to choose which HuggingFace model the server loads. Attackers can reference a malicious repository with a pickle weight file to execute Python code under PyTorch below 2.6, or exhaust disk and memory.	7.5	More Deta
CVE-2026-90869	A remote attacker who knows a valid account's enrolled SSH public key can terminate the shared SSH service in Progress Software WS_FTP Server versions prior to 2024.0.7 and 2025.0.4 on Windows.	7.5	More Deta
CVE-2026-107044	Insecure permissions in ProjectMAXS MAXS Main v0.5.19 (versionCode 19) allows unauthorized attackers to arbitrarily manipulate the app's MAXS command/transport mechanism.	7.5	More Deta
CVE-2026-115713	Improper Link Resolution Before File Access ('Link Following') (CWE-59) in Elastic Cloud Enterprise (ECE) can lead to unauthorized read and write access to data of other deployments on the same host via Symlink Attack (CAPEC-132).	7.5	More Deta
CVE-2026-107047	Insecure permissions in mendhak GPSLogger versionCode 137 allows unauthorized attackers to arbitrarily manipulate the app's logging mechanism and log data.	7.5	More Deta
CVE-2026-	modelscope agent-zero 1.7, 1.8, 1.9, and 1.10 is vulnerable to Directory Traversal in python/helpers/file_browser.py:FileBrowser.save_text_file.	7.5	More

51851	The save_text_file method accepts user-controlled file paths without normalization or validation, allowing path traversal attacks.		Deta
CVE-2026-111418	A server-side request forgery (SSRF) vulnerability exists in the Foxit official website's HTML-to-PDF conversion service. Support for ZIP-formatted input can bypass restrictions on requests to internal IP addresses, potentially allowing discovery of internal network resources.	7.5	More Deta
CVE-2026-111417	A broken access control vulnerability exists in the Foxit official website's HTML-to-PDF conversion service due to the use of a shared token for submitted conversion documents. This may allow unauthorized users to access documents submitted by other users.	7.5	More Deta
CVE-2026-119194	pyasn1 is a generic ASN.1 library for Python. From 0.3.3 until 0.6.5, schemaless container decoding stores every decoded component's TagSet in a growing set even though only one-versus-multiple tag types must be distinguished. Attacker-controlled BER, CER, or DER input contains many distinct long tag IDs whose TagSet hashes collide. Each later set insertion compares against an increasing number of earlier colliding tags in ConstructedPayloadDecoderBase._decodeComponentsSchemaless, producing quadratic CPU work while decoded values and order remain valid. Repeated inputs can exhaust decoder CPU and reduce service availability. This issue is fixed in version 0.6.5.	7.5	More Deta
CVE-2026-9536	A heap-based buffer overflow vulnerability exists in the vtkWindBladeReader FindVariableOffsets functionality of vtk (version(s): 9.6.1). A specially crafted .wind can lead to a buffer overflow. An attacker can provide a malicious file to trigger this vulnerability.	7.5	More Deta
CVE-2026-118659	Happy DOM is a JavaScript implementation of a web browser without its graphical user interface. Prior to 21.0.2, the Happy DOM server-renderer package's ServerRendererServer accepts unauthenticated HTTP/2 requests and resolves attacker-controlled :path values against server.targetOrigin in #onIncomingRequest in packages/@happy-dom/server-renderer/src/ServerRendererServer.ts without confirming that the resolved origin remains trusted before calling fetch. A protocol-relative path can change the destination to an arbitrary HTTP or HTTPS endpoint reachable by the server, including local and internal services, and the proxy relays the fetched response headers and body to the requester. This issue is fixed in version 21.0.2.	7.5	More Deta
CVE-2026-119187	Forge (also called node-forge) is a native implementation of Transport Layer Security in JavaScript. Prior to 1.4.1, the affected implementation used forge.tls.createConnection(), TLS record processing, process() to process the relevant input or security decision. node-forge processed received TLS records recursively, consuming one JavaScript stack frame per record in a single input chunk. A remote peer could send thousands of small records together and exhaust the call stack, causing an uncaught exception and denial of service. This issue is fixed in version 1.4.1.	7.5	More Deta
CVE-2026-119188	Forge (also called node-forge) is a native implementation of Transport Layer Security in JavaScript. Prior to 1.4.1, the affected implementation used forge.tls.createConnection(), fragmented handshake message, interleaved record to process the relevant input or security decision. node-forge continued processing after a TLS record of another content type interrupted a fragmented handshake message. A remote peer could trigger an uncaught TypeError in process(), causing the connection or hosting process to fail. This issue is fixed in version 1.4.1.	7.5	More Deta
CVE-2026-119191	Forge (also called node-forge) is a native implementation of Transport Layer Security in JavaScript. Prior to 1.4.1, the affected implementation used asn1.fromDer(), BIT STRING decoding, maxDepth to process the relevant input or security decision. node-forge decoded ASN.1 stored inside BIT STRING values without consistently applying the configured maxDepth limit and recursively retained copies at each nesting level. Crafted DER containing nested BIT STRINGs could cause excessive recursion, CPU use, and quadratic memory consumption during asn1.fromDer(). This issue is fixed in version 1.4.1.	7.5	More Deta
CVE-2026-118650	Echo is a Go web framework. Prior to 4.16.0 and 5.4.0, a globally mounted middleware.Static instance can interpret an encoded request path differently from Echo's router because the router matches the still-encoded path while the static handler uses the decoded URL.Path. The advisory demonstrates an encoded slash resolving to a file under the static root through the global static middleware, but the source is internally inconsistent about whether a route or group guard protects the corresponding literal path in that global-mount configuration. This issue is fixed in 4.16.0 and 5.4.0.	7.5	More Deta
CVE-2026-119195	pyasn1 is a generic ASN.1 library for Python. Prior to 0.6.5, constructed string and indefinite-length ANY decoding repeatedly concatenates each fragment onto a growing bytes value. Attacker-controlled BER or CER data can use many constructed OCTET STRING or character-string fragments. DER rejects constructed OCTET STRING without a schema, but accepts its definite-length form when asn1Spec selects univ.OctetString; it also accepts constructed character strings such as UTF8String without a schema, even though those encodings are not valid DER. The separate indefinite-length ANY path is reachable in BER and CER when asn1Spec selects univ.Any; DER rejects indefinite lengths. OctetStringPayloadDecoder uses growing header concatenation and AnyPayloadDecoder.indefLenValueDecoder uses growing chunk concatenation, repeatedly copying an increasing prefix and causing quadratic work. A sufficiently fragmented value can occupy decoding workers and cause CPU exhaustion without confidentiality or integrity impact. This issue is fixed in version 0.6.5.	7.5	More Deta
CVE-2026-118772	joi is a schema description language and data validator for JavaScript. From 17.1.1 until 17.13.9 and 18.3.1, the Joi.string().email({ multiple: true }) rule uses a separator regular expression whose leading whitespace quantifier is retried at every position in a long whitespace run that contains no separator, causing quadratic work during String.prototype.split. The behavior applies to the default separator and every custom separator. Applications that validate attacker-controlled values with the multiple option and no effective prior length limit can have the Node.js event loop blocked for seconds by one request, preventing other work. A .max() rule is not sufficient when abortEarly: false allows the email rule to run after the maximum-length check fails. This vulnerability is fixed in versions 17.13.9 and 18.3.1.	7.5	More Deta
CVE-2026-119196	pyasn1 is a generic ASN.1 library for Python. Prior to 0.6.5, constructed BIT STRING decoding repeatedly shifts and copies the complete bit value accumulated from earlier fragments. Attacker-controlled BER or CER input contains many constructed BIT STRING fragments; schema-driven DER also accepts a definite-length constructed BIT STRING. BitStringPayloadDecoder repeatedly calls BitString.fromOctetString with the prior bitString as prepend, shifting an ever-growing SizedInteger for each fragment and causing quadratic work. Large fragmented values can exhaust CPU during decode() without requiring later conversion or formatting. This issue is fixed in version 0.6.5.	7.5	More Deta
CVE-2026-118686	EspoCRM before 9.3.11 and 10.x before 10.0.8 contains a denial of service vulnerability in which the password-redaction regular expression applied during API error handling consumes excessive CPU on long request bodies. Unauthenticated remote attackers can concurrently send a small number of large API requests to exhaust server workers, making EspoCRM slow or unavailable to legitimate users.	7.5	More Deta
CVE-2026-119197	pyasn1 is a generic ASN.1 library for Python. Prior to 0.6.5, binary REAL decoding builds a large mantissa one octet at a time by shifting a growing integer and slicing the remaining byte string. Attacker-controlled ASN.1 includes a binary-encoded REAL with a large mantissa and reaches BER, CER, or DER decode(), with or without a schema containing REAL. RealPayloadDecoder.valueDecoder repeatedly performs a left shift, OR, and suffix copy for every mantissa octet, making decode time quadratic in mantissa length. A comparatively small REAL value can hold a decoding worker on one CPU core for seconds or longer and cause availability loss. This issue is fixed in version 0.6.5.	7.5	More Deta
CVE-2026-118679	n8n before 1.123.83, 2.41.4, and 2.42.1 contains a server-side request forgery vulnerability in the Slack Trigger webhook that allows unauthenticated attackers to exfiltrate Slack tokens by bypassing signature verification when no signing secret is set. Attackers who know the webhook URL can name a file to download, causing the node to send the workspace access token to an attacker host and return the response.	7.5	More Deta
CVE-	Bricks Theme 2.4 and before for WordPress contains an unauthenticated broken access control vulnerability in the load_popup_content REST endpoint that allows anonymous attackers to read draft and unpublished page content by supplying a popupId parameter without any status or		

2026-119325	capability checks. Attackers can obtain a public nonce via the bricks_regenerate_query_nonce action and then increment the popupId value in requests to the /wp-json/bricks/v1/load_popup_content endpoint to enumerate and disclose confidential content from any unpublished post on the site.	7.5	More Deta
CVE-2026-118641	n8n before 1.123.85, 2.x before 2.43.5, and 2.44.x before 2.44.1 contains an OData $filter injection vulnerability in the Microsoft Outlook contact lookup and Microsoft SharePoint v1 item update nodes, which build $filter string literals from expression-bindable parameters without escaping. Attackers who supply untrusted input to such workflows can inject single quotes to dump the bound mailbox's entire contact list or redirect SharePoint writes onto unintended list items within the stored credential's scope.	7.5	More Deta
CVE-2026-118682	KaringX ClashMi through 1.0.32.1801 disables TLS certificate validation by default in the HttpUtils helper, allowing attackers to intercept HTTPS traffic by presenting any certificate. Attackers operating the user's proxy node can serve a forged update manifest omitting sha256 to deliver a malicious installer, achieving code execution when the update runs.	7.5	More Deta
CVE-2026-118689	OvenMediaEngine through 0.21.0 contains a denial of service vulnerability in OvtPacket::LoadHeader() that allows unauthenticated attackers to stall connections by sending payload_length values above 32750. Attackers can send crafted OVT packets to the OVT listener to hold connections open indefinitely and accumulate buffered memory, disrupting origin-to-edge stream relay.	7.5	More Deta
CVE-2026-118694	python-markdown2 through 2.5.5 contains a denial of service vulnerability that allows remote users to exhaust CPU by submitting Markdown with unclosed inline link destinations. Attackers can submit repeated '[a](' or '![a](' sequences, causing _find_balanced to rescan the remaining document for each link and consume quadratic CPU time.	7.5	More Deta
CVE-2026-8824	A memory corruption vulnerability exists in the vtkBMPReader ExecuteDataWithInformation functionality of vtk (version(s): 9.6.1). A specially crafted .bmp file can lead to a buffer overflow. An attacker can provide a malicious file to trigger this vulnerability.	7.5	More Deta
CVE-2026-8822	A memory corruption vulnerability exists in the vtkDEMReader ReadProfiles functionality of vtk (version(s): 9.6.1). A specially crafted USGS DEM can lead to a buffer overflow. An attacker can provide a malicious file to trigger this vulnerability.	7.5	More Deta
CVE-2026-118803	Bricks Theme 2.4.3 and before contains an unauthenticated dynamic-data tag injection vulnerability that allows anonymous attackers to control the urlParams object in the query_result REST endpoint, causing the submitted value to be re-parsed as a Bricks dynamic data tag. Attackers can inject tags such as author_meta:user_pass, author_meta:user_email, or cf_coupon_amount to leak post meta and the post author's user record, including the password hash, without authentication.	7.5	More Deta
CVE-2026-118804	Bricks Builder 2.4.3 and before contains a broken access control vulnerability that allows unauthenticated attackers to access restricted post content by submitting crafted post_status and post_type values in the originalQueryVars parameter to the POST /wp-json/bricks/v1/query_result REST endpoint using a publicly obtainable nonce. Attackers can set post_status to draft or private, or post_type to shop_coupon, to disclose unpublished posts, private content, and WooCommerce coupon data that is otherwise blocked by the standard WordPress REST API routes.	7.5	More Deta
CVE-2026-61569	AVideo is a video-sharing Platform. Prior to 8.1.0, the unauthenticated streamer login at `objects/login.json.php` passes the `user` parameter to `Streamer::get` in `objects/Streamer.php`, where it is interpolated into a single-quoted MariaDB SELECT without parameterization or escaping. Although `objects/security.php` strips literal single quotes, `html_entity_decode` in `objects/Login.php` restores entity-encoded quotes before the query. The supplied `siteURL` must pass the streamer allowlist, which allows all sites when empty by default, and an attacker-hosted login response must set `canUpload` or `isAdmin` to reach `Streamer::createIfNotExists`. That function calls `Streamer::get` before its additional allowlist check. UNION results are exposed through `streamers_id`, while failures return the rendered query and MariaDB error. An attacker can read arbitrary encoder database data, including stored upstream streamer credentials, allowlist configuration, and queue records, without encoder credentials. Stacked statements are not permitted by the mysqli driver and the tested database account lacks global FILE privilege, so the demonstrated vector is bounded to reads rather than server-side file writes. Stolen streamer credentials can provide continued upstream access until rotated. This issue is fixed in version 8.1.0.	7.5	More Deta
CVE-2026-42057	An invalid pointer dereference vulnerability exists in the vtkPNGReader::vtkPNGReaderUpdate2 functionality of vtk 9.6. A specially crafted .png file can lead to a denial of service. An attacker can provide a malicious file to trigger this vulnerability.	7.5	More Deta
CVE-2026-41216	An invalid pointer dereference vulnerability exists in the vtkPNGReader::ExecuteInformation functionality of vtk 9.6. A specially crafted .png file can lead to a denial of service. An attacker can provide a malicious file to trigger this vulnerability.	7.5	More Deta
CVE-2026-119249	A malicious actor with access to the network could exploit a Binding to an Unrestricted IP Address vulnerability found in WiFiman Desktop to obtain information about the host device.	7.5	More Deta
CVE-2026-93757	The Wild Apricot Login plugin for WordPress is vulnerable to Authentication Bypass via SSO Email-Collision Account Binding in all versions up to, and including, 1.0.18. When no WildApricot contact-ID mapping is found for an incoming SSO login, the plugin falls back to a network-global `get_user_by('email', ...)` lookup in `Module.php` to resolve a WordPress user, then `UserSynchronizer::syncWaContact()` binds and `Controller::login()` issues a session cookie via `wp_set_auth_cookie()` for that resolved user — both guarded only by `is_super_admin()` — without ever requiring proof of ownership of the matched WordPress account such as a password, local account-linking confirmation, inbox verification, or administrator approval. This makes it possible for attackers with custom-level WildApricot membership access to authenticate as an existing WordPress subsite administrator on a path-based Multisite network, obtaining a valid network-global authentication cookie for the victim without their credentials. Exploitation requires that the attacker control a WildApricot contact whose email address matches the target WordPress administrator's email — achievable via a public zero-fee membership application on the connected WildApricot organization — and that they complete the SSO flow on any subsite where Wild Apricot Login is active; because WordPress user identities and authentication cookies are network-global, the cookie issued on that subsite is equally valid on any other subsite where the victim user holds an administrator role.	7.5	More Deta
CVE-2026-93855	The SendPress Newsletters plugin for WordPress is vulnerable to time-based SQL Injection via the 'subscriberid' parameter in all versions up to, and including, 1.26.1.20 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. The nonce gating the handler uses the hardcoded action value 'sendpress-is-awesome', which is rendered on the same public page served by the [sp-form formid="manage"] shortcode, making it trivially obtainable by unauthenticated visitors and effectively bypassing the nonce as an access control.	7.5	More Deta
CVE-2026-93904	The Social Web Suite – Social Media Auto Post, Social Media Auto Publish plugin for WordPress is vulnerable to generic SQL Injection via the 'exclude_posts' parameter in all versions up to, and including, 4.1.12 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 HMAC authentication gate protecting the endpoint is bypassable on any freshly activated installation where an administrator has not yet visited the settings page, because the secret_key	7.5	More Deta

	option remains empty until lazily generated at that point, allowing an attacker to compute a valid token using hash_hmac('sha256', '', $timestamp) with any chosen timestamp.		
CVE-2026-118782	Forge (also called node-forge) is a native implementation of Transport Layer Security in JavaScript. Prior to 1.4.1, node-forge accepted a PKCS#12 MAC or PKCS#12 password-based encryption iteration count of zero or less. pki.pbe.generatePkcs12Key() then returned a constant key independent of the password and salt, allowing crafted PKCS#12 input processed by forge.pkcs12.pkcs12FromAsn1() to bypass password-based integrity checks. Predictable encryption keys and IVs also affected PKCS#12 PBE using pbeWithSHAAnd3-KeyTripleDES-CBC or pbewithSHAAnd40BitRC2-CBC, including shrouded key bags, encrypted SafeContents, and PKCS#8 ENCRYPTED PRIVATE KEY input processed independently by forge.pki.decryptPrivateKeyInfo(). PBES2/PBKDF2-encrypted content is unaffected. This issue is fixed in version 1.4.1.	7.5	More Deta
CVE-2026-111739	The Two Factor Authentication WordPress plugin before 1.17.0, All-In-One Security (AIOS) WordPress plugin before 5.5.0 do not bind the account whose two-factor code is verified to the account being authenticated, allowing an attacker who knows a victim's password and holds their own two-factor-enabled account to satisfy the victim's second-factor check with their own code and obtain the victim's session.	7.5	More Deta
CVE-2026-118779	Forge (also called node-forge) is a native implementation of Transport Layer Security in JavaScript. Prior to 1.4.1, the affected implementation used pem.decode(), lib/pem.js, missing END line to process the relevant input or security decision. node-forge used polynomial-time regular expressions in pem.decode(), including when searching for a matching END line and parsing encapsulated headers. An unauthenticated attacker able to supply PEM input to any high-level parser could consume excessive CPU with a long malformed message and cause denial of service. This issue is fixed in version 1.4.1.	7.5	More Deta
CVE-2026-104016	ProtobufParser parses length-prefixed protobuf string and bytes fields by checking (_inputPtr + len) <= _inputEnd and then, on the fast path, calling _finishShortText(len). Both use 32-bit signed integer arithmetic. When an attacker supplies a varint decoding to a length near Integer.MAX_VALUE, _inputPtr + len overflows to a negative value, the bounds check passes, and _finishShortText(len) reaches TextBuffer.expandCurrentSegment(len), which performs Arrays.copyOf with no cap and throws OutOfMemoryError: Requested array size exceeds VM limit. The JVM refuses arrays larger than Integer.MAX_VALUE - 8 before consulting available heap, so -Xmx tuning does not mitigate the issue. StreamReadConstraints.maxStringLength and maxDocumentLength do not gate this path: a 33-byte payload is far below any document-length cap and the string-length check does not fire before the allocation. This was confirmed empirically against shipping artifacts with maxStringLength, maxDocumentLength and maxNestingDepth all configured. A February 2026 hardening commit added the equivalent overflow guard to the packed-array-length and message-length paths but left the string-length call sites unguarded. No privileges or user interaction beyond the ability to submit data for parsing are required.	7.5	More Deta
CVE-2026-107016	Insecure permissions in Fossify v1.3.0 allows unauthorized attackers to access and read another user's stored contacts.	7.5	More Deta
CVE-2026-15323	The Product Designer for WooCommerce WordPress | Lumise plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 2.1.2 via the process_checkout function. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information. The lumise_security nonce required to reach the vulnerable /?lumise=cart endpoint is freely obtainable by any unauthenticated visitor via the /?lumise=ajax action=init handler, making this exploitable with no prior access or credentials.	7.5	More Deta
CVE-2026-116613	The Animated Text Block plugin for WordPress is vulnerable to Sensitive Information Exposure in versions up to, and including, 1.2.6 via the 'animated-text' shortcode. This is due to the atb_shortcode_handler() function fetching an arbitrary post by attacker-supplied ID and, in the 'publish' branch, calling displayContent() with no capability check and no validation that the post's post_type is the plugin's own CPT or is otherwise viewable (is_post_type_viewable()). This makes it possible for authenticated attackers, with Contributor-level access and above, to read the rendered block content of any published post, including posts of non-public custom post types (public=false, show_in_rest=false) that WordPress would otherwise hide from direct URLs and the REST API.	7.5	More Deta
CVE-2026-110747	ProtobufParser._readStringKey() reads the length prefix of a protobuf map entry's string key into an attacker-controlled int and then checks (_inputPtr + len) <= _inputEnd using signed arithmetic. For values near Integer.MAX_VALUE the addition overflows to a negative value and the check passes even when the input contains no key data. The parser then calls _finishShortText(len), which expands the text buffer to the declared length via TextBuffer.expandCurrentSegment and Arrays.copyOf, throwing OutOfMemoryError: Requested array size exceeds VM limit. An 8-byte malformed message containing a map entry with a declared key length of 0x7FFFFFFF is sufficient. Configured StreamReadConstraints, including maxStringLength, maxNameLength, maxDocumentLength and maxNestingDepth, do not prevent the failure. Applications running with -XX:+ExitOnOutOfMemoryError terminate the JVM. This is the same integer-overflow pattern addressed for other call sites in the remediation associated with CVE-2026-104016 and CVE-2026-104017; the map-key call site was corrected on the 3.x branches only, leaving the corresponding 2.x branches unguarded. Release lines 2.18, 2.19 and 2.20 do not contain _readStringKey() and are not affected by this vector. No privileges or user interaction beyond the ability to submit data for parsing are required. The 3.0 release line and 3.1.0-3.1.5 / 3.2.0-3.2.1 do not contain _readStringKey() and are therefore not affected; the method first appears in 3.1.6 and 3.2.2, mirroring its introduction at 2.21.6 on the 2.x side.	7.5	More Deta
CVE-2026-105972	The Menu Cart for WooCommerce WordPress plugin before 3.2.1 does not sanitise and escape cart item variation data before outputting it in its cart slide-out, allowing unauthenticated users to store a Cross-Site Scripting payload that can be delivered to and executed in the session of another user, including a logged-in administrator.	7.5	More Deta
CVE-2026-118377	mews/pos through 2.0.0 contains an insufficient verification of data authenticity vulnerability that allows unauthenticated attackers to forge payment results by submitting unverified callbacks. GarantiPos, PayForPos and InterPos 3D Pay and 3D Host handlers skip check3DHash(), letting attackers post tampered status, amount or order ID fields to complete orders without paying.	7.5	More Deta
CVE-2026-111255	The affiliate-toolkit – Multi-Network Affiliate & Amazon Product Display plugin for WordPress is vulnerable to Arbitrary File Upload in all versions up to, and including, 3.9.2 via the upload_image function. This is due to insufficient file type validation in upload_image due to a weak Content-Type prefix check and extension derivation from the attacker-controlled URL path, with no dangerous-extension stripping. This makes it possible for authenticated attackers, with contributor-level access and above, to upload files that may be executable, which makes remote code execution possible. Exploitation requires the "import product image" option to be enabled in the plugin settings, as this activates the image download pipeline triggered on product post save.	7.5	More Deta
CVE-2026-119128	ZITADEL 4.0.0 before 4.19.5 contains an authentication bypass vulnerability in the Login V2 UI that allows unauthenticated attackers to set the first credential of users lacking any authentication method. Attackers can compute a valid verificationCheck cookie from the user ID and browser fingerprint to set a password, register a passkey, or link an identity provider, taking over the account.	7.4	More Deta
CVE-2026-118205	The Essential Addons for Elementor – Popular Elementor Templates & Widgets plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 6.8.7 via the `page_id` parameter of the `register_user()` function. The vulnerability exists because the handler's post status deny-list rejects `future`, `draft`, and `pending` but admits `inherit` — the status carried by every WordPress revision — allowing an attacker to substitute a revision ID for a live page ID, while a flawed "last saved by administrator" check reads `post_author` on revisions (which reflects the editing administrator) rather than the `_edit_last` meta that is never copied to revisions, and the nonce gate is rendered ineffective because any unauthenticated visitor can freely obtain a valid nonce via the `wp_ajax_nopriv_eael_get_token` endpoint. This makes it possible for unauthenticated attackers to register an account with a role as high as Editor — gaining capabilities including `edit_others_posts`, `publish_pages`, `upload_files`, and `unfiltered_html` — by naming a revision whose `_elementor_data` contains an elevated role an administrator previously saved and later reverted on a page bearing the Login/Register widget. Successful exploitation requires that the site has	7.4	More Deta

	"Anyone can register" enabled and that an administrator has at some point saved and then reverted a non-default "New User Role" on an affected page.		
CVE-2026-119568	vsftpd through 3.0.5 contains an authentication bypass vulnerability in ssl_data_accept() that allows unauthenticated attackers to hijack FTPS data connections by resuming their own TLS session ticket. Attackers sharing the victim's source IP can obtain a ticket via AUTH TLS, then connect to the victim's PASV port to steal downloads or inject upload data.	7.4	More Deta
CVE-2026-6647	In deployments of WSO2 Identity Server configured with a case-insensitive user store and a case-sensitive database for identity data, mismatches in username case handling can occur. This inconsistency results in OAuth token revocation operations failing to correctly identify usernames containing mixed-case characters during certain lifecycle events, preventing tokens from being invalidated. A malicious actor can exploit this vulnerability by possessing a valid access or refresh token associated with a mixed-case username. In affected configurations, these tokens may not be revoked when expected. The actor can then leverage these unrevoked tokens, before their expiry, to continue performing actions that should have been restricted, effectively bypassing intended access controls.	7.4	More Deta
CVE-2026-96187	Access of resource using incompatible type ('type confusion') in Microsoft Edge (Chromium-based) allows an unauthorized attacker to disclose information over a network.	7.4	More Deta
CVE-2026-119190	Forge (also called node-forge) is a native implementation of Transport Layer Security in JavaScript. Prior to 1.4.1, node-forge parsed deprecated extension OIDs 2.5.29.10 and 2.5.29.13 as basicConstraints, and pki.verifyCertificateChain() used the first extension with that name. Exploitation requires a CA trusted by the application to issue a certificate carrying an attacker-supplied deprecated-OID extension, commonly because the CA copies extensions from a certificate signing request. By placing a permissive deprecated extension before the genuine 2.5.29.19 basicConstraints extension, the certificate holder could have the certificate accepted as a CA and issue certificates for arbitrary names, enabling server or client impersonation. If the issuing CA adds a keyUsage extension without keyCertSign, node-forge rejects the chain. This issue is fixed in version 1.4.1.	7.4	More Deta
CVE-2026-118763	sigstore-js provides JavaScript libraries for interacting with Sigstore services. Prior to 0.7.2, packages/oci/src/registry.ts contains a RegistryClient.signIn() method that stores registry Authorization and Docker configuration headers as defaults on a shared HTTP client, while RegistryClient.uploadBlob() sends a fresh PUT to an absolute blob-upload Location supplied by the registry without checking that its origin or scheme matches the registry. A malicious or compromised registry can therefore direct a user pushing an artifact through attachArtifactToImage() to an attacker-controlled host and receive the registry bearer token, Basic credentials, or custom authentication headers. Redirect-time header stripping does not prevent the leak because the cross-host PUT is a new explicit request rather than a followed redirect. This is a residual of CVE-2026-59891, whose fix changed credential selection in credentials.ts but did not constrain where credentials are sent from registry.ts. Version 0.7.2 fixes the issue by separating registry credentials from client-wide defaults and sending them only to the registry origin.	7.4	More Deta
CVE-2026-92092	A flaw was found in openshift-ansible. The installer container's `run` script downloads and executes remote inventory and dynamic scripts without integrity verification. A remote attacker, by performing a Man-in-the-Middle (MITM) attack or compromising the HTTP server providing these scripts, could substitute an arbitrary executable. This malicious executable would then run with the installer's user ID (UID) and full cluster-provisioning privileges, leading to arbitrary code execution.	7.4	More Deta
CVE-2026-114488	A flaw was found in Wildfly. A remote attacker can bypass authentication on IIOP EJB invocations as the CSIv2 security interceptor accepts ITTPrincipalName identity assertions in the service context without verifying transport-level authentication, allowing a pre-auth attacker on the port 3528 to impersonate any principal on every IIOP-exposed @Remote EJB.	7.4	More Deta
CVE-2026-15564	Wildfly's IIOP listener may permit deserialization of input streams before authentication is performed. An attacker who can gain access to the IIOP port may be able to construct and send malicious objects and achieve deserialization, if the target EJB allows untyped method parameters, and depending on the potential gadget chains available in the running classpath.	7.4	More Deta
CVE-2026-119619	A vulnerability was found in 37954679 cak-filemanagement-system up to 5e6433246475e66462e1fea980688de96a049297. This affects the function mysqli_query of the file admin/save_student.php. Performing a manipulation of the argument date/department/subject/forwarded_to/action_taken_by/section/password results in sql injection. The attack is possible to be carried out remotely. The exploit has been made public and could be used. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Deta
CVE-2026-118648	n8n before 1.123.85, 2.x before 2.43.5, and 2.44.x before 2.44.1 contains a stored cross-site scripting vulnerability because some webhook response paths, such as error responses and responses without headers, omit the sandbox Content-Security-Policy. Authenticated members who can create and activate workflows can serve HTML that runs on the n8n origin, letting scripts act with the session of users who open the webhook URL.	7.3	More Deta
CVE-2026-61571	AVideo is a video-sharing Platform. Prior to 8.1.0, the encoder lacks a global authentication layer and exposes control and status PHP endpoints to anonymous network callers. `view/run.php` has a commented-out guard and invokes `Encoder::run()`. `view/queue.json.php` calls `Encoder::getAll(true)`, reveals streamer URLs through `getSiteURL()`, and triggers processing with `execRun()`. `view/status.php` returns `Access-Control-Allow-Origin` with a wildcard, reads the queue, triggers processing, and exposes host memory statistics through `ServerMonitor::getMemory()` when `serverStatus` is set. `view/listFiles.json.php` checks only `Login::canBulkEncode()`, which admits anonymous callers whenever `disableBulkEncode` is empty, the default. Its `path` parameter is resolved with `realpath()` and listed with `scandir()` without a base-directory restriction. An unauthenticated attacker can drive the privileged queue processor, read queue and streamer-site information, obtain memory statistics and enumerate media file names and paths in any directory readable by the web-server user. Enumeration is limited to configured media extensions and does not itself disclose arbitrary file contents. This issue is fixed in version 8.1.0.	7.3	More Deta
CVE-2026-6064	Link following vulnerability in Data Shredder components in Norton Antivirus, Avast Antivirus, and AVG Internet Security prior to 26.5.10933 on Windows allows a local, low-privileged attacker to escalate privileges to SYSTEM. During a privileged shred operation, enabling arbitrary file/folder deletion that is leveraged to gain NT AUTHORITY\SYSTEM privelages.	7.3	More Deta
CVE-2026-91912	Dell OpenManage Enterprise, versions prior to 4.8.0, contains an Use of Hard-coded Cryptographic Key vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information disclosure.	7.3	More Deta
CVE-2026-119620	A vulnerability was determined in 37954679 cak-filemanagement-system up to 5e6433246475e66462e1fea980688de96a049297. This vulnerability affects the function move_uploaded_file of the file admin/add_logs.php. Executing a manipulation of the argument File can lead to unrestricted upload. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Deta
CVE-2026-99122	In the Linux kernel, the following vulnerability has been resolved: vsock/vmci: validate packet source for connected sockets vmci_transport_recv_stream_cb() looks up sockets first by the full source and destination tuple, then by destination only in the bound table. The fallback can select a non-listening socket without checking whether the packet came from its stored peer. This was reproduced with two VMCI contexts. A RST from the context not stored in a TCP_SYN_SENT socket reset that socket after it was selected by the destination-only lookup. VMCI can process notification packets in bottom-half context when the socket is not owned by user context, or defer packets to a workqueue. Use vsock_check_source() after taking the socket lock in the bottom-half path, and recheck after lock_sock() in the workqueue path. Listening sockets	7.3	More Deta

	continue to accept packets from any source. Reply with a RST addressed from the received packet before dropping a source that fails validation. This preserves the existing reset behavior for bound non-listening and concurrently closed sockets without directing the reset to a connected socket's stored peer.		
CVE-2026-62848	Metalama is a Roslyn-based open-source patterns and architecture toolkit for C#. From 2023.0.101-rc until 2025.1.18, 2026.0.25 and 2026.1.19, the Windows Visual Studio integration deserializes local named-pipe messages without restricting which CLR types can be instantiated. The pipe connects `devenv`, the out-of-process Roslyn code-analysis process and the `CodeLens` process, and has the predictable name `Metalama_{role}_{processId}_{hash(PackageVersion)}`. Releases from the first public 2023.0 line through 2026.0.x use Newtonsoft.Json with `TypeNameHandling.All`; the later `SerializationBinder` only remaps assembly names, and `BindToType` resolves arbitrary wire-supplied types without an allow-list. Releases 2026.1.0 through 2026.1.18 use typeless MessagePack with `TypelessObjectResolver` and likewise instantiate arbitrary types. A same-user local process able to write to the pipe can send crafted messages that lead to arbitrary code execution with confidentiality, integrity and availability impacts inside the affected Visual Studio process. Default Windows pipe ACLs limit writers to the same logged-in user, so this does not escalate privileges or cross a security boundary; command-line and MSBuild-only builds do not use the channel. The maintained Metalama + PostSharp extension is affected from 2024.1 through 2026.1.4, while earlier Metalama-free PostSharp versions are unaffected. The retired Metalama and Caravela extensions remain affected and require removal or migration. The framework issue is fixed in versions 2025.1.18, 2026.0.25 and 2026.1.19; the maintained Metalama + PostSharp Visual Studio extension is fixed in version 2026.1.5. The retired Metalama and Caravela extensions require removal or migration.	7.3	More Deta
CVE-2026-116869	Shop manager PHP Object Injection in myPOS Checkout <= 1.4.5 versions.	7.2	More Deta
CVE-2026-118078	Shop manager PHP Object Injection in Product Catalog Feed by PixelYourSite <= 3.1.4 versions.	7.2	More Deta
CVE-2026-118077	Author PHP Object Injection in Sastra Essential Addons for Elementor <= 1.2.3 versions.	7.2	More Deta
CVE-2026-116390	Deserialization of Untrusted Data vulnerability in stepasyuk Filter Everything — WordPress & WooCommerce Filters filter-everything allows Object Injection.This issue affects Filter Everything — WordPress & WooCommerce Filters: from n/a through 1.9.7.	7.2	More Deta
CVE-2026-116865	Editor PHP Object Injection in Zippy <= 1.7.0 versions.	7.2	More Deta
CVE-2026-118074	Shop manager PHP Object Injection in Finale Lite <= 2.21.0 versions.	7.2	More Deta
CVE-2026-116864	Author PHP Object Injection in WPCargo Track & Trace <= 8.0.5 versions.	7.2	More Deta
CVE-2026-118079	Deserialization of Untrusted Data vulnerability in FolioVision FV Flowplayer Video Player fv-wordpress-flowplayer allows Object Injection.This issue affects FV Flowplayer Video Player: from n/a through 7.5.56.7212.	7.2	More Deta
CVE-2026-118238	The Tenda W18E web management server is vulnerable to OS command injection via the "diagnose" packet-capture feature due to improper validation of JSON fields. An authenticated user can inject shell metacharacters into the protocol or targetDevice fields, which are later concatenated into a tcpdump command and executed with root privileges. This vulnerability can be exploited without authentication if the device is in a factory-reset state.	7.2	More Deta
CVE-2026-115708	Improper Link Resolution Before File Access ('Link Following') (CWE-59) in Elastic Cloud Enterprise (ECE) can lead to authentication bypass and unauthorized changes to the configuration of other deployments on the same host via Symlink Attack (CAPEC-132).	7.2	More Deta
CVE-2026-115590	Deserialization of Untrusted Data vulnerability in weDevs Dokan dokan-lite allows Object Injection.This issue affects Dokan: from n/a through 5.3.1.	7.2	More Deta
CVE-2026-96741	The DSGVO All in one for WP plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Comment Content via Output Buffer Regex Corruption in all versions up to, and including, 5.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This is only exploitable when the administrator has enabled both the 'Google Tag Manager' integration and the 'Replace integration automatically [Beta]' option, and requires the crafted comment to be approved by an administrator.	7.2	More Deta
CVE-2026-115301	The Contact Form by Supsystic WordPress plugin before 1.11.1 does not sandbox the template engine used to render its forms and allows stored form-editor content to reach that engine as executable template code, enabling an administrator to perform server-side template injection and execute arbitrary code on the server. The injected template is compiled and executed whenever any visitor loads a page containing the form, so the stored payload also lets an unauthenticated visitor read server-side secrets such as authentication salts and database credentials.	7.2	More Deta
CVE-2026-107743	The Mapster WP Maps plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to, and including, 2.0.5. This is due to the /wp-json/mapster-wp-maps/save-mapmaker REST route being registered with a permission_callback that unconditionally returns true (no capability check, no nonce), together with the mapster_write_config_to_acf() helper only sanitizing string config values with sanitize_text_field() — which strips HTML tags but leaves quote characters intact — and the mapster_wp_map shortcode renderer in mapster_wordpress_maps_shortcode_display() concatenating the stored loading_background_color value into a single-quoted inline style attribute without esc_attr(). 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 Deta
CVE-2026-54453	OpenCATS is an open-source applicant tracking system and recruitment CRM for staffing agencies and hiring teams. Prior to version 0.10.0, the Professional License configuration feature in `SettingsUI` (`manageProfessional`) accepts administrator-controlled license key input that is reconstructed into a PHP `define()` statement in `config.php` without safe escaping. Because the application includes `config.php`, crafted input can alter the file's PHP syntax and cause persistent arbitrary PHP execution with the web server process privileges. An authenticated administrator must have Settings module access and permission to update Professional License configuration, and `config.php` must be writable for this write-	7.2	More Deta

	based path. Successful exploitation can read, modify or delete application data, expose candidate, contact, company, job order and user account information, alter the installation or configuration, and provide a foothold for further attacks. Unauthenticated exploitation and exploitation without Settings access are not established. This issue is fixed in version 0.10.0.		
CVE-2026-116392	Deserialization of Untrusted Data vulnerability in PickPlugins Accordion accordions allows Object Injection.This issue affects Accordion: from n/a through 2.3.25.	7.2	More Deta
CVE-2026-118755	Volmarg Personal Management System through 2.1.0 contains an OS command injection vulnerability that allows authenticated users to execute shell commands via unescaped folder paths in the storage module's tree command. Attackers can create a directory under upload/files containing shell metacharacters such as $(...) and then move or copy it, running commands as the web server user.	7.2	More Deta
CVE-2026-111577	The GoSMTP WordPress plugin before 1.2.5 does not perform a settings-management authorization check on its SMTP configuration page, which is gated only on the GoSMTP WordPress plugin before 1.2.5-activation capability, allowing users with a delegated role below administrator to change outbound mail delivery and achieve administrator account takeover.	7.2	More Deta
CVE-2026-33923	A signature verification vulnerability was discovered in the update installation functionality due to inconsistent validation of the update bundle contents. An attacker with administrative privileges can remotely supply a crafted update bundle that passes signature verification but runs an unsigned script when the bundle is installed. The script runs with root privileges, allowing the attacker to read or modify sensitive data, change the appliance configuration, or shut down the appliance.	7.2	More Deta
CVE-2026-117607	Xerte Online Toolkits through 3.15.5 contains a remote code execution vulnerability that allows authenticated users with system permission to run PHP by importing a crafted language pack. Attackers can upload a ZIP via import_language.php containing a .inc file, then request it through the language parameter to execute code on the server.	7.2	More Deta
CVE-2026-33924	Two OS command injection vulnerabilities were discovered in the update installation functionality due to insufficient validation of the update bundle contents. An attacker with administrative privileges can remotely supply a crafted update bundle that, when installed, causes arbitrary commands to be executed with root privileges, allowing the attacker to read or modify sensitive data, change the appliance configuration, or shut down the appliance.	7.2	More Deta
CVE-2026-115821	The NewsmanApp plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'billing_first_name, billing_last_name' parameter in all versions up to, and including, 3.7.29 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This vulnerability is only exploitable when the Newsman Remarketing feature is enabled and a non-empty Remarketing ID is configured in the plugin settings.	7.2	More Deta
CVE-2026-96666	The Schema App Structured Data plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Comment Content via 'Remove Microdata' Output Filter 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. Exploitation requires that an administrator has enabled the plugin's 'Remove Microdata' option and approves the malicious comment.	7.2	More Deta
CVE-2026-96767	The NEX-Forms – Ultimate Forms Plugin for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'type' parameter in all versions up to, and including, 9.3.2 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.	7.2	More Deta
CVE-2026-111314	The affiliate-toolkit – Multi-Network Affiliate & Amazon Product Display plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'atkp_product_producturl' parameter in all versions up to, and including, 3.9.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Exploitation by unauthenticated attackers requires that the plugin's AJAX loading / AJAX handler option is enabled (atkp_options::get_ajax_loading_enabled() || get_ajax_handler_enabled()) and the attacker knows a product id to render. On a default installation, where that is not configured, the vulnerability requires attackers with contributor-level access and above.	7.2	More Deta
CVE-2026-109999	The AI Marketing Expert — AI Email Marketing, AI Content Generator, SEO Analyzer, AI Workflow Automation, Social Media & Ai Chatbot plugin for WordPress is vulnerable to Stored DOM-Based Cross-Site Scripting via the 'name' parameter in all versions up to, and including, 1.2.8 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 only that the chatbot module is active with at least one configured bot; the attacker stores the payload via three unauthenticated REST calls, and the JavaScript widget auto-poll then delivers it to any administrator who opens wp-admin/index.php.	7.2	More Deta
CVE-2026-118257	Vue I18n is the internationalization plugin for Vue.js. From 11.1.10 until 11.4.14 and from 12.0.0-alpha.4 until 12.0.0-alpha.5, sanitizeTranslatedHtml() escapes markup and event-handler text inside an iframe srcdoc value but leaves the srcdoc attribute active. Browsers decode the character references and parse the value as a same-origin nested HTML document, allowing attacker-controlled parameters or translation content placed in srcdoc to execute script when applications enable escapeParameter and render translations as HTML through v-html. Versions 9.14.5 and 10.0.8 are also affected and are no longer supported, while i18n-t rendering is not affected. This issue is fixed in versions 11.4.14 and 12.0.0-alpha.5.	7.2	More Deta
CVE-2026-96669	The Food Store – Online Food Delivery & Pickup plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'service_type' Cookie in all versions up to, and including, 1.5.5 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The attack is seeded unauthenticated by supplying a payload via the ?type= query parameter on the public checkout page, which the plugin writes directly into the browser's service_type cookie; this cookie value is later persisted to order meta and rendered unescaped in the admin panel.	7.2	More Deta
CVE-2026-86393	Dell PowerProtect Data Domain, Feature Release versions 7.7.1.0 through 8.8, LTS2024 release versions 7.13.1.0 through 7.13.1.80, LTS2025 release versions 8.3.1.0 through 8.3.1.40, LTS2026 release versions 8.6.1.0 through 8.6.1.20, contain an Improper Privilege Management vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Elevation of privileges.	7.2	More Deta
CVE-2026-11587	SQL injection allowing an authenticated user with access to ACL management to read and modify the Centreon database	7.2	More Deta
CVE-2026-86399	Dell PowerProtect Data Domain, Feature Release versions 7.7.1.0 through 8.8, LTS2024 release versions 7.13.1.0 through 7.13.1.80, LTS2025 release versions 8.3.1.0 through 8.3.1.40, LTS2026 release versions 8.6.1.0 through 8.6.1.20, contain an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Command execution.	7.2	More Deta
CVE-2026-86379	Dell PowerProtect Data Domain Management Center, Feature Release versions 7.7.1.0 through 8.8, LTS2024 release versions 7.13.1.0 through 7.13.1.80, LTS2025 release versions 8.3.1.0 through 8.3.1.40, LTS2026 release versions 8.6.1.0 through 8.6.1.20, contain an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A high privileged attacker with remote access	7.2	More Deta

	could potentially exploit this vulnerability, leading to Command execution.		
CVE-2026-86380	Dell PowerProtect Data Domain, Feature Release versions 7.7.1.0 through 8.8, LTS2024 release versions 7.13.1.0 through 7.13.1.80, LTS2025 release versions 8.3.1.0 through 8.3.1.40, LTS2026 release versions 8.6.1.0 through 8.6.1.20, contain an Integer Overflow or Wraparound vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Protection mechanism bypass.	7.2	More Deta
CVE-2026-97645	The Gravity Forms plugin for WordPress is vulnerable to Stored Cross-Site Scripting via List Field in all versions up to, and including, 3.1.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Successful exploitation requires the administrator to click the injected link in the entry detail view and confirm a dialog, which triggers the admin JavaScript bundle's delegated data-dialog-callback handler to invoke the attacker-supplied function reference.	7.2	More Deta
CVE-2013-20007	Linksys WAG200G through 1.01.06 contains an OS command injection vulnerability that allows authenticated attackers to execute commands by injecting backtick-delimited input into the timer_interval parameter. Attackers can send a crafted POST request to setup.cgi to start telnetd or download and run a backdoor, gaining full device control.	7.2	More Deta
CVE-2026-86389	Dell PowerProtect Data Domain, Feature Release versions 7.7.1.0 through 8.8, LTS2024 release versions 7.13.1.0 through 7.13.1.80, LTS2025 release versions 8.3.1.0 through 8.3.1.40, LTS2026 release versions 8.6.1.0 through 8.6.1.20, contain an Integer Overflow or Wraparound vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Code execution.	7.2	More Deta
CVE-2026-86394	Dell PowerProtect Data Domain, Feature Release versions 7.7.1.0 through 8.8, LTS2024 release versions 7.13.1.0 through 7.13.1.80, LTS2025 release versions 8.3.1.0 through 8.3.1.40, LTS2026 release versions 8.6.1.0 through 8.6.1.20, contain an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Command execution.	7.2	More Deta
CVE-2026-101210	Dell OpenManage Enterprise, versions prior to 4.8.0, contains an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Command execution.	7.2	More Deta
CVE-2026-90437	The Gravity Forms plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Post Excerpt / Post Custom Field / Rich-Text Paragraph Field Values in all versions up to, and including, 3.1.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This is possible because Post Excerpt, Post Custom Field, and Rich-Text-Editor-enabled Paragraph Text fields allow raw HTML submissions via allow_html(), and an entity-encoded payload stored in a data-dialog-confirm attribute evades wp_kses_post() at save time but is decoded into executable markup by the browser when the plugin's admin JavaScript passes the attribute value to insertAdjacentHTML().	7.2	More Deta
CVE-2026-116622	The Food Store – Online Food Delivery & Pickup plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'service_time' parameter in all versions up to, and including, 1.5.5 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 the site to have the 'Enable Checkout Service Fields' option turned off, which is a non-default configuration, while 'Enable Pickup/Delivery Service' remains enabled.	7.2	More Deta
CVE-2026-101214	Dell OpenManage Enterprise, versions prior to 4.8.0, contains an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Command execution.	7.2	More Deta
CVE-2026-111504	Dell OpenManage Enterprise, versions prior to 4.8.0, contains an Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Elevation of privileges.	7.2	More Deta
CVE-2026-86395	Dell PowerProtect Data Domain Virtual Edition, Feature Release versions 7.7.1.0 through 8.8, LTS2024 release versions 7.13.1.0 through 7.13.1.80, LTS2025 release versions 8.3.1.0 through 8.3.1.40, LTS2026 release versions 8.6.1.0 through 8.6.1.20, contain an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Command execution.	7.2	More Deta
CVE-2026-96894	The ERP: Complete HR, Accounting & CRM Suite Built for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Inbound Email Body in all versions up to, and including, 1.17.10 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The inbound email router's only gate is a regex match on the References header for a reply token whose hash is never cryptographically validated, meaning any external party who received or can mimic a CRM outbound email can satisfy the check without a WordPress account.	7.2	More Deta
CVE-2026-119409	OPNsense before 26.7.8 contains a command injection vulnerability that allows authenticated users with the System: Firmware privilege to execute commands as root by storing a malicious firmware mirror URL. Attackers can submit shell metacharacters through POST /api/core/firmware/set that opnsense-update evaluates with eval, and can also disable package signature verification through sed injection.	7.2	More Deta
CVE-2026-104744	The Independent Analytics Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'utm_campaign' parameter in all versions up to, and including, 2.15.5 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 the Independent Analytics Pro build to be active, as the free build nulls campaign parameters; additionally, the attacker must first visit a frontend page to obtain a server-signed payload that can be replayed with a crafted utm_campaign value against the unauthenticated /iawp/search REST endpoint, since the signature check does not cover utm_* fields.	7.2	More Deta
CVE-2026-42701	Shop manager PHP Object Injection in YayMail <= 4.4.6 versions.	7.2	More Deta
CVE-2026-110541	Dell PowerProtect Data Domain, Feature Release versions 7.7.1.0 through 8.8, LTS2024 release versions 7.13.1.0 through 7.13.1.80, LTS2025 release versions 8.3.1.0 through 8.3.1.40, LTS2026 release versions 8.6.1.0 through 8.6.1.20, contain an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to command execution.	7.2	More Deta
CVE-2026-112365	The easy.jobs – AI powered Job Listing, Job Board, Career Page, Recruitment & Hiring Solution plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'cover_letter' parameter in all versions up to, and including, 2.8.4 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Successful execution requires an administrator to open the affected candidate's Application tab and click the attacker-crafted link, at which point WHATWG URL parsing collapses the encoded scheme back to javascript: and executes the payload.	7.2	More Deta

CVE-2026-111111	The Prime Slider – Hero Slider, Carousel, WooCommerce & Post Slider Elementor Addons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'comment' parameter in all versions up to, and including, 4.7.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This is possible because core wp_filter_kses leaves the submitted markup inert, but the plugin's subsequent regex fallback consumes closing quotes of allowed attribute values containing 'bdt-', promoting previously inert bytes — such as event handlers like onfocus — into real HTML attributes that are then written to the database and rendered without further sanitization.	7.2	More Deta
CVE-2026-97019	The AMP for WP – Accelerated Mobile Pages plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'headline-*' Shortcode Attribute in all versions up to, and including, 1.1.17 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. A Subscriber-level user can store a malicious shortcode in their biographical info field; because WordPress core's wp_filter_kses() only strips HTML tags and not shortcode syntax, and because AMP content sanitizers run before do_shortcode() processes the archive description, the synthesized markup is never post-sanitized.	7.2	More Deta
CVE-2026-118089	Shop manager PHP Object Injection in Product Feed Manager <= 7.14.1 versions.	7.2	More Deta
CVE-2026-110662	The MxChat – AI Chatbot & Content Generation for WordPress plugin for WordPress is vulnerable to Stored DOM-Based Cross-Site Scripting via the 'feedback' parameter in all versions up to, and including, 3.2.25 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 stored payload is written by any unauthenticated visitor via a single POST to admin-ajax.php and detonates automatically when any administrator next loads the Transcripts page.	7.2	More Deta
CVE-2026-109381	The Mage Eventpress plugin for WordPress is vulnerable to privilege escalation in versions up to, and including, 5.7.8 This is due to the mep_grant_shop_manager_access() function hooking user_has_cap and unconditionally granting manage_options whenever an attacker-controllable request marker matches — most notably $_GET['page'] starting with 'mep_' or 'mpwem_', which is never validated against an actually registered EventPress screen. This makes it possible for authenticated attackers, with Shop Manager-level access and above, to elevate their privileges to Administrator by appending ?page=mep_x to core admin URLs (options-general.	7.2	More Deta
CVE-2026-116851	Unauthenticated Cross Site Scripting (XSS) in eCommerce Product Catalog <= 3.6.5 versions.	7.1	More Deta
CVE-2026-115596	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in impleCode eCommerce Product Catalog ecommerce-product-catalog allows Reflected XSS.This issue affects eCommerce Product Catalog: from n/a through 3.6.4.	7.1	More Deta
CVE-2026-115612	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in iova.mihai SliceWP slicewp allows Stored XSS.This issue affects SliceWP: from n/a through 1.2.13.	7.1	More Deta
CVE-2026-115593	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 2.0.24.	7.1	More Deta
CVE-2026-115609	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Stiofan GetPaid invoicing allows Stored XSS.This issue affects GetPaid: from n/a through 2.8.62.	7.1	More Deta
CVE-2026-115606	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Crowd Favorite DXP ToolKit dxp-toolkit allows Stored XSS.This issue affects DXP ToolKit: from n/a through 2.0.1.	7.1	More Deta
CVE-2026-67187	Ninja Forms plugin for WordPress before 3.15.4 contains an incomplete server-side validation vulnerability that allows unauthenticated attackers to submit arbitrary values to Checkbox List, Multi-Select List, Image List, Country, and State fields because NF_Abstracts_List falls through to a validate() method that only checks required-field presence. Attackers can submit crafted formula payloads through the unauthenticated nf_ajax_submit endpoint that bypass CSV escaping applied only to Textbox and Textarea fields, resulting in CSV injection when an administrator downloads and opens the exported submissions file.	7.1	More Deta
CVE-2026-103411	An Integer Underflow vulnerability in DhcpMessageDecoder in Juniper Networks Session Smart Router allows an attacker with local network access to cause information disclosure and a denial of service via a malicious DHCP reply.	7.1	More Deta
CVE-2026-116847	Unauthenticated Cross Site Scripting (XSS) in Mang Board WP <= 2.4.6 versions.	7.1	More Deta
CVE-2026-59164	NORA is a self-hosted artifact registry and pull-through cache. Prior to 0.9.5, `nora-registry` authenticates the token-management UI but fails to require administrator authorization. `auth_middleware()` protects `/ui/tokens` and `/api/ui/tokens`, but state-changing requests are checked only with `role.can_write()`, not `role.can_admin()`. `tokens_page()` and `tokens_list()` call `store.list_all_tokens()`, exposing IDs and metadata across all users, while `tokens_revoke()` calls `store.revoke_token` using the supplied token ID without an ownership or admin check. A read bearer token can enumerate other users' token existence, owner, role, description, expiry and last-use metadata. A write bearer token or write-capable OIDC identity can additionally revoke arbitrary admin and service tokens, disrupting the registry and forcing credential recovery. Read-only identities cannot POST a revocation. This issue is fixed in version 0.9.5.	7.1	More Deta
CVE-2026-118038	In Progress® Telerik® Document Processing Libraries prior to version 2026.3.1027, a path traversal vulnerability in the Convert and Merge AI agent tools allows an authenticated attacker with low privileges who can supply tool arguments to read files outside the configured output directory, and to overwrite such files where they are writable, via relative file paths that resolve against the process current working directory.	7.1	More Deta
CVE-2026-119707	SonicJS through 3.0.0 contains a missing authorization vulnerability in the /api/:collection and /api/content write routes that only check coarse role labels. Authenticated authors or editors can use a bearer JWT or API key to create, modify, publish, or soft-delete other users' documents, bypassing document ACLs and administrator deny overrides.	7.1	More Deta
CVE-2026-54855	Unauthenticated Cross Site Scripting (XSS) in Profile Builder <= 4.0.5 versions.	7.1	More Deta

CVE-2026-48201	Unauthenticated Cross Site Scripting (XSS) in Fast Velocity Minify <= 3.5.7 versions.	7.1	More Deta
CVE-2026-39786	Unauthenticated Cross Site Scripting (XSS) in BA Book Everything <= 1.8.33 versions.	7.1	More Deta
CVE-2026-119710	PipesHub 0.3.0 before 0.10.0 contains an event type injection vulnerability that allows authenticated users with only the crawl:write scope to delete connectors by injecting into the :connector path segment. Attackers can send a :connector value like web.delete to the schedule route, bypassing connector:delete and lock checks to remove connector instances and purge record embeddings.	7.1	More Deta
CVE-2026-118642	n8n before 1.123.85, 2.43.5, and 2.44.1 contains an authorization bypass vulnerability that allows authenticated members to use inaccessible credentials through inline sub-workflow nodes with non-boolean disabled values. Attackers knowing a credential id can run Execute Workflow nodes in inline JSON mode that skip the permission check and send decrypted credentials to attacker-controlled servers.	7.1	More Deta
CVE-2026-28160	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in e4jvikwp VikRentCar vikrentcar allows Stored XSS.This issue affects VikRentCar: from n/a through 1.4.10.	7.1	More Deta
CVE-2026-118675	n8n before 1.123.85, 2.43.5, and 2.44.1 contains a credential guard bypass vulnerability that allows editors of shared workflows to use restricted credentials by loading sub-workflows from URLs or local files. Attackers can configure the Execute Sub-workflow node with source url or localFile to serve content that resolves project credentials and returns their decrypted values.	7.1	More Deta
CVE-2026-111021	The افزونه پیامک ووکامرس | Persian WooCommerce SMS WordPress plugin before 7.3.2 does not sanitise and escape a parameter before reflecting it back into an HTML attribute, leading to Reflected Cross-Site Scripting that is executed in the browser session of a logged-in privileged user who is tricked into submitting a crafted cross-site request.	7.1	More Deta
CVE-2026-118676	n8n before 1.123.85, 2.43.5, and 2.44.1 contains an authorization bypass vulnerability that allows member users to use credentials they cannot access by omitting default node parameters. Attackers can save and run workflows where pre-execution checks skip credential slots, causing decrypted credential values to be sent to attacker-chosen destinations.	7.1	More Deta
CVE-2026-118678	n8n before 2.41.4 and 2.42.x before 2.42.1 contains a prototype pollution vulnerability that allows low-privileged users to alter built-in object behaviour by saving workflows with specially named connection keys. Attackers can add keys such as __proto__ to workflow connections, which the periodic history compaction task processes, causing logins and writes to fail with server errors.	7.1	More Deta
CVE-2026-119289	Zuke is a code-first, strongly typed build automation system for Deno. Prior to 1.10.0, the @zuke/gh githubWorkflow(...) gate correlates a dispatched workflow run using only a display-title marker that is visible in the workflow run list and can be copied by another dispatcher. In configurations where the external workflow repository grants workflow_dispatch permission to a party not equally trusted by the releasing repository, an attacker can dispatch a run with the marker and cause the gate to adopt its conclusion without verifying the event, ref, or creation window. A passing substituted run can authorize an unvalidated release, while a failed or cancelled run can block a valid release, and the persisted adopted run ID preserves the substitution across build resume. This issue is fixed in version 1.10.0.	7.1	More Deta
CVE-2026-52729	Xibo is an open source digital signage platform with a web content management system and Windows display player software. Prior to 4.4.3, missing access-control checks on `PUT/DELETE /action/{id}` allow an authenticated user to modify or delete actions on any Layout. Exploitation requires the privilege to allow edits, including deletion, to all created Layouts, which is granted to non-administrators as standard. This issue concerns `Layout actions` rather than the separately reported DataSet export vulnerability. This issue is fixed in version 4.4.3.	7.1	More Deta
CVE-2026-105077	Unauthenticated Cross Site Scripting (XSS) in Ad Inserter <= 2.8.19 versions.	7.1	More Deta
CVE-2026-116405	Unauthenticated Cross Site Scripting (XSS) in VikRentCar <= 1.4.9 versions.	7.1	More Deta
CVE-2026-99112	In the Linux kernel, the following vulnerability has been resolved: net/sched: cls_flower: validate mask pointer after nla_next() fl_set_enc_opt() iterates the key's nested tunnel-option attributes with nla_for_each_attr() while advancing a single mask pointer via nla_next() at the bottom of each loop, so the mask cursor is driven by the number of key attributes rather than by the mask's own attributes. The nla_ok() added by commit c96adff956191 ("cls_flower: call nla_ok() before nla_next()") only validates the mask pointer that was just consumed; the pointer produced by nla_next() is used by the next iteration (fl_set_geneve_opt() and siblings) without any validation. The mask's nested attributes are validated with NL_VALIDATE_LIBERAL, which merely warns on trailing bytes that do not form a complete attribute. A mask carrying one valid attribute plus 1-3 residue bytes (or a non-aligned attribute length making msk_depth negative) therefore reaches the next iteration with msk_depth != 0, so neither the !msk_depth check in fl_set_enc_opt() nor the !depth check in the per-type helpers fires. nla_type() then reads past the mask payload and nla_parse_nested_deprecated() iterates with an nla_len taken from those bytes, reading well beyond the mask attribute (KASAN: slab-out-of-bounds read in __nla_validate_parse from fl_change()). Validate the advanced mask pointer as well: when the mask is not legitimately exhausted (msk_depth != 0) and the new pointer fails nla_ok(), reject the filter with -EINVAL. An exactly exhausted mask still skips the check, preserving exact-match behaviour for the remaining key attributes.	7.1	More Deta
CVE-2026-116409	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Swings Upsell Order Bump Offer for WooCommerce upsell-order-bump-offer-for-woocommerce allows Reflected XSS.This issue affects Upsell Order Bump Offer for WooCommerce: from n/a through 3.1.6.	7.1	More Deta
CVE-2026-111503	Dell OpenManage Enterprise, versions prior to 4.8.0, contains an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Information exposure.	7.1	More Deta
CVE-2026-117609	rtl_433 through 25.12 contains a stack-based buffer overflow vulnerability in proflame2_mc() that allows nearby attackers to write past a 7-byte stack buffer by sending more than seven valid Manchester-coded words. Attackers can transmit a crafted OOK radio signal or supply a crafted signal file to crash rtl_433 and corrupt stack memory, enabling control-flow hijacking on builds without stack canaries.	7.1	More Deta
CVE-2026-61993	Unauthenticated Cross Site Scripting (XSS) in Blockonomics 3.11.0 versions.	7.1	More Deta
CVE-2026-99142	In the Linux kernel, the following vulnerability has been resolved: tracing: Check operator stack capacity before pushing predicate_parse() uses the first operator stack entry before processing any opening parentheses. A push then increments top before writing. The existing check still permits that write when top already points to the last allocated entry, which can access beyond the operator stack. Reject the push when top	7.1	More Deta

	reaches the last allocated entry.		
CVE-2026-119331	Ladybird is a truly independent web browser. Prior to the c0d68bddf3e3616e5173835f0f4c155ee9700d91 commit, CSSStyleSheet.cssRules, insertRule(), and deleteRule() in Libraries/LibWeb/CSS/CSSStyleSheet.cpp did not enforce the stylesheet origin-clean flag with the required SecurityError, even though cross-origin imported stylesheets were correctly marked non-origin-clean. A malicious page could read parsed rules from a stylesheet loaded without CORS and could insert or delete rules in the victim stylesheet, bypassing the Same-Origin Policy. Reading could expose selectors, generated content, feature markers, or other sensitive rule text, while mutation could alter page visibility or layout. The issue does not provide memory corruption, code execution, or persistence after the attacker page closes. This vulnerability is fixed by commit c0d68bddf3e3616e5173835f0f4c155ee9700d91.	7.1	More Deta
CVE-2026-110540	Dell PowerProtect Data Domain Management Center, Feature Release versions 7.7.1.0 through 8.8, LTS2024 release versions 7.13.1.0 through 7.13.1.80, LTS2025 release versions 8.3.1.0 through 8.3.1.40, LTS2026 release versions 8.6.1.0 through 8.6.1.20, contain a Missing Authorization vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Unauthorized operation.	7.1	More Deta
CVE-2026-119337	RAGFlow is an open-source RAG (Retrieval-Augmented Generation) engine. From 0.25.2 until 0.27.3, POST /api/v1/agents/chat/completions invokes completion_openai and returns through the openai-compatible branch before UserCanvasService.accessible() checks whether the caller may access the requested agent. An authenticated user who knows another user's private agent UUID can execute that Only me workflow and read its output across the user or tenant boundary; configured tools may also cause side effects, but stronger impacts were not demonstrated. This issue is fixed in version 0.27.3.	7.1	More Deta
CVE-2026-119407	Element Web and Element Desktop before 1.12.32 accept guest credentials from URL fragment parameters in loadSession, allowing remote unauthenticated attackers to log out users and clear local stores. Attackers can lure logged-in users into opening links with guest_user_id and guest_access_token to force an attacker-controlled guest session and destroy unbacked end-to-end encryption keys.	7.1	More Deta
CVE-2026-108494	Unauthenticated Cross Site Scripting (XSS) in Chained Quiz <= 1.4.1 versions.	7.1	More Deta
CVE-2026-118085	Unauthenticated Cross Site Scripting (XSS) in GlobalPayments WooCommerce <= 1.23.3 versions.	7.1	More Deta
CVE-2026-119549	Jellyfin through 12.4 contains a server-side request forgery vulnerability that lets authenticated users bypass SvgSecurityValidator by embedding gzip-compressed SVG in non-SVG image data URIs. Attackers can upload such profile images via POST /UserImage, then trigger unauthenticated rendering via GET /UserImage to fetch internal URLs, read local image files, or exhaust memory.	7.1	More Deta
CVE-2026-27394	Unauthenticated Cross Site Scripting (XSS) in Eventer <= 0.1.1 versions.	7.1	More Deta
CVE-2026-61995	Unauthenticated Cross Site Scripting (XSS) in YouTube Showcase <= 4.1.0 versions.	7.1	More Deta
CVE-2026-42692	Unauthenticated Cross Site Scripting (XSS) in WP Crowdfunding <= 2.2.2 versions.	7.1	More Deta
CVE-2026-54864	Unauthenticated Cross Site Scripting (XSS) in Post Video Players <= 1.165 versions.	7.1	More Deta
CVE-2026-54866	Unauthenticated Cross Site Scripting (XSS) in Razorpay Payment Button Elementor Plugin <= 1.2.8 versions.	7.1	More Deta
CVE-2026-61988	Unauthenticated Cross Site Scripting (XSS) in Auction Nudge – Your eBay on Your Site <= 8.4.0 versions.	7.1	More Deta
CVE-2026-86715	Plaintext storage of a password vulnerability in Crypttech Crypto and Informatics Technologies Industry and Trade Inc. Vatos DLP allows Use of Known Domain Credentials. This issue affects Vatos DLP: from 1.1.176 before 1.1.243.	7.1	More Deta
CVE-2026-61989	Unauthenticated Cross Site Scripting (XSS) in Easy Property Listings <= 3.5.25 versions.	7.1	More Deta
CVE-2026-91914	Dell OpenManage Enterprise, versions prior to 4.8.0, contains an Authentication Bypass by Spoofing vulnerability. An unauthenticated attacker with adjacent network access could potentially exploit this vulnerability, leading to Session theft.	7.1	More Deta
CVE-2026-115592	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in OceanWP OceanWP oceanwp allows Reflected XSS.This issue affects OceanWP: from n/a through 4.2.7.	7.1	More Deta
CVE-2026-63184	Refitter is a tool for generating a C# REST API client using the Refit library. Prior to 2.1.1, the `refitter` dotnet tool invokes `NJsonSchema` with unsafe defaults for `$ref` resolution when generating Refit interfaces and contracts from attacker-controlled or attacker-influenced OpenAPI descriptions. Remote `http(s)` references cause requests from the developer or CI host and inline untrusted remote schema content into generated output. Absolute local file paths and relative `../` traversal outside the input directory also resolve and inline local content, permitting arbitrary local-file disclosure. The demonstrated chain stops at server-side request forgery, remote file inclusion, and local file inclusion, not code execution: Refit sets the base URL at runtime, enum values use verbatim-string doubling, and string defaults are escaped. This issue is fixed in version 2.1.1.	7.1	More Deta
CVE-2026-63286	Database backups are vulnerable to offline attacks. Backups created using a version prior to the patched version are still vulnerable. AXIS Camera Station Pro automatically creates one more such backup for recovery purpose when the update is applied. Delete all these backups and change the credentials stored in AXIS Camera Station Pro.	7.1	More Deta

CVE-2026-99123	In the Linux kernel, the following vulnerability has been resolved: vsock/virtio: validate packet source for connected sockets virtio_transport_recv_pkt() looks up sockets first by the full source and destination tuple, then by destination only in the bound table. The fallback is needed for listening and connecting sockets, but sockets remain in the bound table after connect(), so it can also return a non-listening socket. The fallback does not validate the source address. In TCP_SYN_SENT, a RESPONSE from an unrelated source can transition the victim socket to TCP_ESTABLISHED while its stored remote address remains unchanged. Subsequent RW packets from that source are delivered through the same destination-only fallback. This was reproduced with capability-empty processes under different UIDs. The attacker discovered the target tuple through unprivileged AF_VSOCK sock_diag and caused the victim socket to read 16 attacker-chosen bytes; the intended peer-side socket read 0 of those 16 bytes. Add vsock_check_source() to validate the transport, source port and source CID against the peer stored in a non-listening socket. The local transport is the CID exception because its packets are generated internally with VMADDR_CID_LOCAL as their source, including connections using CID aliases. Use the helper after lock_sock() in the virtio receive path.	7.1	More Deta
CVE-2026-94175	Unauthenticated Cross Site Scripting (XSS) in All In One Login <= 2.4.1 versions.	7.1	More Deta
CVE-2026-119649	Orchard CMS 1.10.3 through 1.11 contains an improper authorization vulnerability in MediaLibraryService.CheckMediaFolderPermission() that allows authenticated Authors and Contributors to access other users' media. Attackers can display, clone, and delete other users' media items by content id and delete arbitrary media folders via FolderController.Delete().	7.1	More Deta
CVE-2026-115963	Missing Authorization vulnerability in VideoWhisper.com Broadcast Live Video videowhisper-live-streaming-integration allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Broadcast Live Video: from n/a through 7.3.9.	7.1	More Deta
CVE-2026-115611	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PluginUs.Net TableOn posts-table-filterable allows Reflected XSS.This issue affects TableOn: from n/a through 1.0.7.	7.1	More Deta
CVE-2026-112827	Missing Authorization vulnerability in VillaTheme HANDMADE – Dropshipping for Etsy and WooCommerce handmade-dropshipping-for-etsy-and-woo allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects HANDMADE – Dropshipping for Etsy and WooCommerce: from n/a through 1.0.10.	7.1	More Deta
CVE-2026-99110	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix heap overflow in cifs_do_set_acl() cifs_set_acl() validates ACL size using posix_acl_xattr_size(): 4 + (count * 8) // 4-byte header + 8 bytes per ACE cifs_do_set_acl() then calls posix_acl_to_cifs() to write the CIFS wire format into the same buffer: 6 + (count * 10) // 6-byte header + 10 bytes per ACE An ACL that passes the xattr-based check in cifs_set_acl() can overflow the heap when posix_acl_to_cifs() writes the larger CIFS format. Validate the CIFS format size against the remaining buffer space and USHRT_MAX before converting--data_count is __u16, so sizes above USHRT_MAX truncate the on-wire packet length, causing the server to apply a partial ACL. Replace MaxDataCount = 1000 with min(CIFSMaxBufSize, USHRT_MAX).	7.0	More Deta
CVE-2026-99212	In the Linux kernel, the following vulnerability has been resolved: net/rds: don't let the rdma_cm destroy an id RDS still owns on route failure rds_rdma_cm_event_handler_cmn() hands the return value of rdma_resolve_route() straight back to the rdma_cm on RDMA_CM_EVENT_ADDR_RESOLVED. A synchronous failure there - -ENOMEM from the route work allocation, an SA query that cannot be set up, a RoCE route with no usable device - makes addr_handler() destroy the id the event was delivered on. That id is ic->i_cm_id, and nothing clears the pointer: the connection sits in RDS_CONN_CONNECTING with a freed id until its shutdown calls rdma_disconnect() and rdma_destroy_id() on it. The ROUTE_RESOLVED case already avoids this: rds_ib_cm_initiate_connect() forces a zero return while ic->i_cm_id == cm_id, as the comment there explains. Do the same here - drop the connection and return 0 - so the id stays RDS's to destroy from the shutdown, and the reconnect gets a fresh one.	7.0	More Deta
CVE-2026-118905	Node Version Manager (nvm) is a POSIX-compliant shell function for managing multiple node.js versions. In versions 0.31.2 through 0.40.5, `nvm_ls` filters installed versions with a sed program that embeds the requested version pattern in a `\#...#` address, escaping `.` (and, since 0.40.4, `#`) but not backslash. A version string containing `#` (or `\#`) therefore closes the address early, and the rest of it is parsed as sed commands: with GNU sed, the `e` command runs a shell command as the user; with BSD sed, the `w` and `r` commands write and read files. This is reachable whenever an attacker-influenced version string is passed to `nvm use`, `nvm which`, `nvm ls`, `nvm version`, `nvm run`, or `nvm exec`, or to `nvm-exec` via `NODE_VERSION`, and at least one version is installed. nvm's own `.nvmrc` parser strips comments, so a bare `nvm use` is not affected; however, the bash `cdnvm` and zsh `load-nvmrc` auto-switch hooks documented in the README read `.nvmrc` as-is and pass it to `nvm ls` and `nvm version`, so a user with one of those hooks installed runs the attacker's command just by changing into a directory under a malicious `.nvmrc`; scripts that run `nvm use "$(cat .nvmrc)"` are affected the same way. Version 0.40.6 passes any version pattern containing `#` or a newline through the `.nvmrc` content parser first, so no `#` reaches the sed program.	7.0	More Deta
CVE-2026-99136	In the Linux kernel, the following vulnerability has been resolved: dm-crypt: fix a tiny race condition in crypt_dec_pending crypt_dec_pending reads io->error before calling atomic_dec_and_test. Another context, for example crypt_endio called from an interrupt, may set io->error and drop its reference between the read and the decrement. crypt_dec_pending then drops the last reference and completes the bio with the stale status - so a read that failed and was never decrypted, or a write that failed, is reported as successful. The read was placed before the decrement by commit b35f8caa0890 ("dm crypt: wait for endio to complete before destruction"), because that commit freed dm_crypt_io before calling bio_endio. This is no longer the case, dm_crypt_io lives in the per-bio data now. Read io->error after atomic_dec_and_test instead. atomic_dec_and_test is fully ordered, so no additional barrier is needed.	7.0	More Deta
CVE-2026-84243	The gettext family of functions in the GNU C Library version 2.0 and later accept LANGUAGE environment variable entries that contain '/' or that are equal to "..", unless the program is setuid or setgid (AT_SECURE). An attacker who can set LANGUAGE in the environment of a program that uses gettext can make it load a message catalog (.mo file) from an arbitrary location in the file system. A crafted .mo file can crash the program through out-of-range offsets, or supply translations whose format directives do not match the arguments passed by the program. That causes undefined behaviour in the printf family of functions and may allow arbitrary code execution with the privileges of the program. The safety of message catalogs relies on them being installed in trusted, read-only locations, and the directory traversal bypasses this. The fix for CVE-2014-0475 rejects ".." path components in locale names passed to setlocale or taken from the LC_ALL, LC_* and LANG environment variables. gettext reads LANGUAGE directly and appends each colon-separated entry to the message catalog directory, so that fix did not cover LANGUAGE. LANGUAGE is only used when the LC_MESSAGES locale is not "C", "C.<encoding>" or "POSIX", so the attacker must also be able to select another installed locale, for example through LANG or LC_ALL. Exploitation also requires that the attacker can place the crafted file in a location readable by the target program, and that the environment crosses a trust boundary without the program running as AT_SECURE. An example is an SSH server that accepts LANGUAGE and LANG from clients through the AcceptEnv directive and restricts an account to a forced command; the attacker may use this to escape the restriction.	7.0	More Deta
CVE-2026-99148	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: keep the eviction fence until the last handle is closed amdgpu_gem_object_close() detaches the user queue eviction fence from the BO before it checks bo_va->ref_count, so closing any handle of a BO removes the fence, even when the file still has another handle to the BO and the bo_va with its GPU mappings stays. The BO can then be evicted without suspending the user queues of the file, which keep accessing it through mappings that are only marked for update. Seen on navi31 with a SDMA user queue: a BO opened twice in the same file (GEM_FLINK + GEM_OPEN) loses its eviction fence when the second handle is closed (traced attach/detach of the fence): attach bo=ffff8c78a6c84c00 GEM_CLOSE handle=7 detach bo=ffff8c78a6c84c00 while handle 6 and the mapping are	7.0	More Deta

	still in use. Only detach the fence when the last reference to the bo_va goes away, matching amdgpu_gem_object_open(), which attaches it only when the bo_va is created. With this the fence stays until the file is closed. (cherry picked from commit 8387982f03d4026b7dc11b0b5e3118298eee4d6a)		
CVE-2026-118692	CherryTree through 1.7.2 contains an OS command injection vulnerability in CtActions::link_clicked that allows attackers to execute commands by embedding shell metacharacters in web link URLs. When the non-default Custom Web Link Clicked Action option is enabled, attackers can supply crafted documents whose links pass $(...), backticks, or semicolons unquoted to std::system, running commands as the victim on click.	7.0	More Deta
CVE-2026-119288	Zuke is a code-first, strongly typed build automation system for Deno. Prior to 1.51.0, @zuke/core launches resolved Windows .cmd and .bat shims by prepending cmd /c, causing cmd.exe to reparse a command line assembled with C-runtime quoting rules. A build running on Windows that resolves a tool from node_modules/.bin and passes attacker-influenced text containing an unquoted &, |, or ^ metacharacter can execute an additional attacker-chosen command in the build's context with access to its credentials. POSIX platforms are not affected. This issue is fixed in version 1.51.0.	7.0	More Deta
CVE-2026-84296	Multi-Factor Authentication Bypass vulnerability in SSH component in Progress Software WS_FTP Server versions prior to 2024.0.6, and 2025.0.3 on Windows allows authenticated users to bypass MFA requirements through improper association of authentication factors between accounts.	6.8	More Deta
CVE-2026-119424	OPNsense core before 26.7.8 contains a configuration line injection vulnerability that allows authenticated users with wireless-edit privilege to inject directives by embedding CR/LF characters in WPA fields. Attackers can place newlines in wpa.identity, wpa.passphrase, or RADIUS shared secrets to append arbitrary wpa_supplicant or hostapd directives loaded by root-run daemons.	6.8	More Deta
CVE-2026-86383	Dell PowerProtect Data Domain, Feature Release versions 7.7.1.0 through 8.8, LTS2025 release versions 8.3.1.0 through 8.3.1.40, LTS2026 release versions 8.6.1.0 through 8.6.1.20, contain an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Information disclosure.	6.8	More Deta
CVE-2026-119764	Mythic 3.2.16 through 3.4.0.61 contains a stored cross-site scripting vulnerability that allows attackers controlling target endpoint files to run JavaScript in the Mythic UI origin by planting HTML in .pdf-named files. When an operator downloads the file and clicks Preview Media, content-sniffed HTML from /direct/view renders same-origin, stealing localStorage JWTs for full GraphQL and REST access.	6.8	More Deta
CVE-2026-104694	The Thrive Automator WordPress plugin before 11.2 does not properly sanitize and escape a parameter's array key before using it in a SQL query, allowing authenticated attackers with editor-level access to perform blind SQL injection attacks.	6.8	More Deta
CVE-2026-118165	The Firelight Lightbox WordPress plugin before 2.3.23 does not escape the URL of links it opens in its Classic lightbox before inserting it into the page as HTML, which could allow users with a role as low as Contributor to perform Stored Cross-Site Scripting attacks against users who click a crafted link.	6.8	More Deta
CVE-2026-118071	The Joinchat WordPress plugin before 6.4.2 does not escape the message of its button block before outputting it in an HTML attribute on the front end, which could allow users with the Author role and above to perform Stored Cross-Site Scripting attacks against any visitor of the post, including administrators.	6.8	More Deta
CVE-2026-113488	The GeoDirectory WordPress plugin before 2.8.196 does not properly escape a post badge shortcode attribute for a JavaScript context before placing it in an inline event handler, allowing users with the Contributor role and above to perform Stored Cross-Site Scripting attacks against anyone who clicks the badge, including administrators.	6.8	More Deta
CVE-2026-107098	The Royal Addons for Elementor WordPress plugin before 1.7.1070 does not sanitise and escape one of its map widget's size settings before concatenating it into an HTML attribute, allowing users with the Contributor role or above to inject JavaScript that runs in the browser of any user who views the page, including an administrator reviewing a pending submission.	6.8	More Deta
CVE-2026-93006	A flaw was found in dnsmasq. The TFTP server can serve the wrong file contents because a recently used transfer cache is not invalidated when a transfer finishes. An attacker on the local network who can request a TFTP file may cause a later client to receive previously cached data instead of the requested file. In PXE network-boot environments this can substitute attacker-chosen boot content for a victim machine.	6.8	More Deta
CVE-2026-113487	The GeoDirectory WordPress plugin before 2.8.196 does not properly sanitise or escape a post badge click-through link value before outputting it in an anchor element on a listing, allowing users with the Contributor role and above to perform Stored Cross-Site Scripting attacks against higher-privileged users who view the listing, including an administrator reviewing moderated content.	6.8	More Deta
CVE-2026-110505	The Enable SVG, WebP, and ICO Upload WordPress plugin before 1.1.6 does not prevent animation elements in uploaded SVG files from changing a link's target to a javascript: URI, which could allow users with the author role and above to bypass its SVG sanitization and perform Stored Cross-Site Scripting attacks that execute in WebKit-based browsers such as Safari.	6.8	More Deta
CVE-2026-111967	The MP3 Audio Player WordPress plugin before 5.16 does not escape one of its audio player shortcode attributes before outputting it into an HTML attribute, allowing users with Contributor-level access and above to inject arbitrary JavaScript that executes when another user, such as an administrator previewing a pending post, views the content.	6.8	More Deta
CVE-2026-91915	Dell OpenManage Enterprise, versions prior to 4.8.0, contains an Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') vulnerability. A high privileged attacker with adjacent network access could potentially exploit this vulnerability, leading to Script injection.	6.8	More Deta
CVE-2026-116641	The DB Tools rely on the TLS implementation in Golang’s standard library, which generally uses the system CA store. However, the crypto/x509 package also has its own internal denylist of known-bad CA certificates. Golang 1.27.3 adds the eMudhra certificates to this list. DB Tools version 100.19.0 was compiled with Golang 1.26.8, which does not include this check. The issue is resolved by updating to Golang 1.27.3 in DB Tools 100.20.0	6.8	More Deta
CVE-2026-111027	The Welcart e-Commerce WordPress plugin before 2.12.6 does not properly sanitise and escape a parameter before using it in a SQL query, and strips the escaping it had applied before running the query, allowing users with the Editor role or higher to perform SQL injection attacks.	6.8	More Deta
CVE-2026-119577	ArcadeDB before 26.10.2 contains an improper authorization vulnerability that allows revoked users to retain access through already-open Postgres, Bolt, MongoDB, or Redis wire-protocol connections. Attackers holding an existing connection can keep reading and writing data after deletion, grant removal, or password rotation, because executors keep a stale ServerSecurityUser.	6.8	More Deta
CVE-2026-110524	The Copy Anything to Clipboard for WordPress WordPress plugin before 5.5.5 does not sanitize and escape a shortcode attribute before storing it and writing it back into the page through a client-side script, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks against higher-privileged users who view and interact with the content.	6.8	More Deta
CVE-	The Page Builder by SiteOrigin WordPress plugin before 2.38.0 does not sanitize or escape a widget property before storing it and outputting it in		More

2026-110506	the page builder interface, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks against higher-privileged users who open the affected post in the editor.	6.8	Deta
CVE-2026-93008	A flaw was found in dnsmasq. When following a CNAME in a DNS response, the resolver can cache records for the CNAME target without checking that those records belong to the responding server's authorized zone. In split-DNS deployments that send some domains to a specific upstream, an attacker who controls that upstream can inject cache entries for unrelated names. Later clients may then receive attacker-chosen addresses for those names.	6.8	More Deta
CVE-2026-118425	A flaw was found in the secure-redirect-uris-enforcer client policy of Keycloak, an identity and access management solution. The issue occurs when the policy is configured to allow loopback addresses, as Keycloak resolves hostnames via DNS during validation. An attacker can bypass domain allowlist restrictions by using a hostname that resolves to a loopback address, potentially allowing the registration of unauthorized redirect URIs.	6.8	More Deta
CVE-2026-115683	A race condition in Epiphany allows a malicious website to bypass the TLS/SSL certificate warning page. Epiphany registers the main-world script message handler "tlsErrorPage" so its internal TLS error page can implement "Accept Risk and Proceed". The handler was registered immediately before loading the error page, leaving a brief window where the previously loaded untrusted origin could still call window.webkit.messageHandlers.tlsErrorPage.postMessage(...). The only authorization check compares a numeric WebKit page id that increments predictably; an attacker can burst-guess ids and approve a certificate exception with no user click. If a victim visits malicious site A that redirects to site B with an invalid certificate, site A can, for a few milliseconds, disable TLS certificate error warnings for host B until Epiphany is restarted, enabling man-in-the-middle or site spoofing for that host. Upstream report: https://gitlab.gnome.org/GNOME/epiphany/-/work_items/2978 Proof of concept: https://beford.net/poc/ssl_poc.html Fix: https://gitlab.gnome.org/GNOME/epiphany/-/merge_requests/2245 (register handlers on LOAD_COMMITTED). No fixed release tagged yet; reporter and maintainer describe all current versions as affected. Maintainer notes the risky registration timing dates to commit 1da1caed (Epiphany 45.x era); before that the handlers were always registered and similarly reachable from web content.	6.8	More Deta
CVE-2026-119704	Bastille through 1.4.4 contains a symlink following vulnerability in the cp.sh, rcp.sh and jcp.sh subcommands that allows jailed users to escape jail isolation. Attackers inside a jail can plant symlinks pointing to host paths or other jail roots, so administrator-run copies overwrite or read host files with root privileges.	6.8	More Deta
CVE-2026-115706	Authorization Bypass Through User-Controlled Key (CWE-639) in Elastic Cloud Enterprise (ECE) can lead to privilege escalation via Privilege Abuse (CAPEC-122). An attacker who controls any host in an ECE installation can obtain credentials that are reserved for other platform roles. These credentials can give the attacker full control of the ECE control plane and of the deployments that it manages.	6.8	More Deta
CVE-2026-110504	The Enable SVG, WebP, and ICO Upload WordPress plugin before 1.1.6 does not sanitize uploaded SVG files whose content is not detected as SVG, while still storing and serving them as SVG images, which could allow users with the author role and above to perform Stored Cross-Site Scripting attacks.	6.8	More Deta
CVE-2026-119561	phpMyAdmin through 5.2.3 contains an authentication bypass vulnerability in CustomServer::parseAndValidateAssertionResponse() that never verifies WebAuthn assertion signatures against stored public keys. Attackers holding a victim's MySQL credentials can POST a crafted webauthn_request_response with matching challenge, origin, and rpIdHash to bypass the second factor and gain database privileges.	6.8	More Deta
CVE-2026-103404	An Incorrect Permission Assignment for Critical Resource vulnerability in RoutingManager in Juniper Networks Session Smart Conductor allows a local user to access sensitive routing credentials via triggering processes that write to the /tmp directory.	6.8	More Deta
CVE-2026-115281	The Recipe Card Blocks Lite WordPress plugin before 3.6.4 does not sanitize and cast a block and shortcode attribute before concatenating it into SQL queries, allowing authenticated users with Contributor-level access or above to perform SQL injection attacks.	6.8	More Deta
CVE-2026-119343	Stirling-PDF is a locally hosted web application that facilitates various operations on PDF files. Prior to 3.0.0, POST /api/v1/ai/tools/create-pdf-from-html-agent accepts attacker-controlled htmlContent and passes it to WeasyPrint without CustomHtmlSanitizer, unlike the sanitized /api/v1/convert/html/pdf control path. HTTP and HTTPS resource references can make server-side requests to internal or cloud-metadata destinations, while file references can embed local content readable by the Stirling-PDF process into the generated PDF. The endpoint is reachable without credentials when security.enableLogin is false, and the flaw is distinct from earlier Stirling-PDF WeasyPrint vulnerabilities in older conversion paths. This issue is fixed in version 3.0.0.	6.8	More Deta
CVE-2026-116248	In pgAdmin 4 server mode only administrators are meant to share a server with all users; the server dialog shows the Shared switch only to them. The create and update endpoints of the server API, however, stored the "shared" flag and shared username they were sent, so any user able to register a server could share one with every other user. The servers.json import had a similar gap: a non-administrator's "Shared" entries were removed only after validation, so a file that also held an invalid entry could create a shared server. A shared server carries no credentials, so this gives no direct access. It lets a user plant a server, named to look trusted, in every other user's tree and pointing at a host the user controls; anyone who then connects to it presents their own database password to that host. The fix refuses a non-administrator's request that would share a server with HTTP 403, prunes a non-administrator's shared entries from a servers.json import before validating it, and warns at startup about servers shared earlier by non-administrators. This issue affects pgAdmin 4: before 9.19.	6.8	More Deta
CVE-2013-20008	Linksys WAG200G through 1.01.06 contains a weak password change mechanism that allows attackers to change the administrator password without supplying the current password. Attackers with access to an authenticated administrator browser session can set a new password to lock out the legitimate administrator and take persistent device control.	6.8	More Deta
CVE-2026-90720	Dell PowerProtect Data Domain, Feature Release versions 7.7.1.0 through 8.8, LTS2024 release versions 7.13.1.0 through 7.13.1.80, LTS2025 release versions 8.3.1.0 through 8.3.1.40, LTS2026 release versions 8.6.1.0 through 8.6.1.20, contain an Improper Validation of Integrity Check Value vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Protection mechanism bypass.	6.7	More Deta
CVE-2026-119251	A malicious actor with local access and high privileges could exploit an Improper Access Control vulnerability found in WiFiman Desktop for macOS to escalate privileges on the host device.	6.7	More Deta
CVE-2026-90861	Progress Software WS_FTP Server versions prior to 2024.0.7 and 2025.0.4 on Windows may expose a user's password in clear text to another administrator, who could use it to gain broader administrative access to the server.	6.6	More Deta
CVE-2026-90872	Improper neutralization of directives in dynamically evaluated code in the Manager web console of Progress Software WS_FTP Server versions prior to 2024.0.7 and 2025.0.4 on Windows could allow an authenticated Manager administrator to execute arbitrary commands with the privileges of the WS_FTP Server IIS worker process.	6.6	More Deta
CVE-	Chamilo LMS is an open-source learning management system. In the 1.x line before 1.11.40, and the 2.x line before 2.0.1, multiple `eval()` calls in the vendored PEAR `HTML_QuickForm` libraries can execute arbitrary PHP code if form element names contain attacker-influenced data. Standard		

2026-44344	Chamilo forms use hardcoded element names; exploitation requires a developer-specific plugin or misconfiguration that lets user input reach those element names. Where that conditional path exists, the impact can be full server compromise. This issue is fixed in versions 1.11.40 and 2.0.1.	6.6	More Deta
CVE-2026-58458	Don't Starve Together (Steam AppID 322330) through build 747465 contains a memory-corruption vulnerability in the native persistent-string decoder that allows a remote attacker operating a public dedicated server to crash a victim's game client by publishing crafted world_gen_data with an invalid Klei persistent blob header length. Attackers can craft a malicious public lobby server listing that, once viewed or selected by the victim, triggers client-side decoding of the attacker-controlled data to corrupt native memory and cause a remote denial of service.	6.5	More Deta
CVE-2026-62300	Filecoin Pin is an IPFS Pinning Service API implementation that pins to Filecoin's PDP service. In daemon deployments up to and including version 1.1.0, `POST /pins` in `src/filecoin-pinning-server.ts` checks a caller-supplied CID with `CID.parse` and passes it to `pinStore.pin`, but does not enforce request rate limits or per-user quotas. In `src/filecoin-pin-store.ts`, each pin independently schedules `_processPinInBackground` with `setTimeout` without a queue, semaphore or concurrency cap, then recursively traverses the full DAG using `helia.pins.add(cid)`. The per-pin Helia/Bitswap node in `src/create-pinning-helia.ts` has no application-level byte, block or traversal-time limits. Blocks are written under `carStoragePath` by `src/core/car/car-blockstore-base.ts` and `src/core/car/car-file-backend.ts`, with `stats.totalSize` updated only after writing. An authenticated caller, or an anonymous caller when `ALLOW_NO_AUTH=true`, can submit large DAGs and exhaust disk, network, CPU, memory and libp2p resources, causing service degradation or host/process failure and leaving partial CAR files requiring recovery. The default localhost binding and token requirement reduce exposure. Because nodes have no bootstrap or mDNS configuration, a CID alone may not be fetchable, but caller-supplied `origins` can point to a reachable attacker-controlled libp2p source; concurrent requests accelerate resource pressure. Version 1.1.1 documents operational mitigations but does not implement the missing resource controls.	6.5	More Deta
CVE-2026-51902	SuperAGI up to v0.0.14 contains an improper access control vulnerability. The agent controller endpoint /api/agents/get/project/{project_id} allows authenticated users from one organization to retrieve the complete list of agents belonging to a different organization's project. The endpoint accepts a project_id parameter but does not verify that the project belongs to the authenticated user's organization.	6.5	More Deta
CVE-2026-116404	Missing Authorization vulnerability in David Anderson Redux Framework redux-framework allows Lifting Sensitive Data Embedded in Cache.This issue affects Redux Framework: from n/a through 4.5.16.	6.5	More Deta
CVE-2026-118760	Kubeflow Pipelines enables users to build and deploy portable, scalable machine learning workflows. From 0.5.1 until 2.17.0, the frontend artifact routes did not check whether an authenticated user was authorized to access the requested namespace. A user who can reach the frontend and knows an artifact location can select another tenant's namespace, or omit the namespace and reach an unguarded direct handler, to read artifact contents such as datasets, models, or pipeline outputs. The issue applies to multi-user deployments that rely on Kubeflow Pipelines authorization for tenant isolation. Authentication at ingress identifies the caller but does not authorize access to the selected artifact namespace. The issue does not establish arbitrary Kubernetes Secret disclosure, storage modification, or server-side code execution. This issue is fixed in version 2.17.0.	6.5	More Deta
CVE-2026-118757	PiWeb Disable payment method / Partial payment for WooCommerce before 1.1.10.9 contains a missing authorization vulnerability in the update_fees AJAX handler that allows unauthenticated attackers to modify and read other customers' orders. Attackers can reuse a nonce from their own order-pay page and supply sequential order_id values to change payment methods, recalculate fees, and disclose order line items and totals.	6.5	More Deta
CVE-2026-113485	The Media Library Assistant WordPress plugin before 3.42 does not consistently validate its CSRF nonce on the Media Library bulk-action handler, checking the nonce only when its field is present, so a forged request that omits the field can cause a logged-in user with the Author role or above to trash or delete attachments.	6.5	More Deta
CVE-2026-115957	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Discussion Board WP Discussion Board wp-discussion-board allows Stored XSS.This issue affects WP Discussion Board: from n/a through 2.6.0.	6.5	More Deta
CVE-2026-65444	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Creative Themes Blocksy Companion blocksy-companion allows Stored XSS.This issue affects Blocksy Companion: from n/a through 2.1.60.	6.5	More Deta
CVE-2026-113486	The Media Library Assistant WordPress plugin before 3.42 does not verify a CSRF nonce on its Empty Trash media action, so a forged cross-site request can cause a logged-in user with the Editor role or above to permanently delete every trashed attachment on the site.	6.5	More Deta
CVE-2026-82411	Open Object provides an API and admin interface to manage objects and object types. From 2.4.3 until 2.5.1, 3.6.2, 4.0.2, and 4.1.1, a token scoped to read one ObjectType can read the full versioned record of an object of any other ObjectType via the history-detail endpoint `GET /api/v2/objects/{uuid}/{index}`. The `history_detail` action in `src/objects/api/v2/views.py` calls `self.get_queryset()` and `get_object_or_404` directly instead of `self.get_object()`, so `check_object_permissions` and the per-object check in `ObjectTypeBasedPermission.has_object_permission` are not invoked. The queryset's `filter_for_token` applies only to the list and search actions, while `ObjectTypeBasedPermission.has_permission` allows non-create actions, leaving neither check to constrain history-detail records to the token's permitted ObjectType. The normal retrieve endpoint returns 403 for the same unauthorized object, and the sibling history action enforces the grant. Any valid non-superuser API token with a read grant on at least one ObjectType can therefore disclose another ObjectType's complete versioned object `data`, which can include citizen or case records and sensitive identifiers in government deployments. This issue is fixed in versions 2.5.1, 3.6.2, 4.0.2, and 4.1.1.	6.5	More Deta
CVE-2025-12523	Broken Object Level Authorization in Users Configuration Endpoint allows Information Disclosure to authenticated user	6.5	More Deta
CVE-2026-119148	Incomplete string validation in AWS aws-nitro-enclaves-sdk-c before 0.4.6 may allow a third party to impersonate the AWS KMS endpoint. To remediate this issue, users should rebuild any custom enclave image against aws-nitro-enclaves-sdk-c 0.4.6.	6.5	More Deta
CVE-2026-45141	Chamilo LMS is an open-source learning management system. Prior to 2.0.1, the `add`, `delete_gradebook_from_skill`, `save_profile`, and `delete_profile` actions in `public/main/inc/ajax/skill.ajax.php` perform database mutations without `Security::check_token()` validation. An attacker can use cross-site request forgery to cause an authenticated administrator or DRH who visits a malicious page to create, modify, or delete skill records and profiles, or remove skill-gradebook associations. This issue is fixed in version 2.0.1.	6.5	More Deta
CVE-2026-90991	IBM Langflow OSS 1.0.0 through 1.12.4 could allow a remote authenticated attacker to cause a denial of service due to allocation of resources without limits or throttling.	6.5	More Deta
CVE-2026-	The PayPlug for WooCommerce (Official) WordPress plugin before 3.1.1 does not perform any capability or ownership check on a set of unauthenticated AJAX actions that operate on a caller-supplied order identifier, allowing unauthenticated attackers to modify, read the contents of,	6.5	More

113813	and permanently delete arbitrary WooCommerce orders.		Deta
CVE-2026-59993	Picotls is a TLS protocol library that allows users select different crypto backends based on their use case. In affected revisions through 44bc503, when picotls is used as a `client-side TLS stack`, a peer can send a `HelloRetryRequest` followed by a `spoofed Hello message` that causes a null-pointer dereference. This can terminate the consuming process, including a process performing other work, resulting in denial of service. This issue is fixed in commit a06ca41.	6.5	More Deta
CVE-2026-77819	IBM Langflow OSS 1.0.0 through 1.12.3 could allow a remote authenticated attacker to overwrite arbitrary files due to improper limitation of a pathname to a restricted directory.	6.5	More Deta
CVE-2026-77817	IBM Langflow OSS 1.0.0 through 1.12.4 could allow a remote authenticated attacker to obtain sensitive information due to improper sanitization of secrets during flow and project exports.	6.5	More Deta
CVE-2026-118661	Happy DOM is a JavaScript implementation of a web browser without its graphical user interface. Prior to 20.14.6, Happy DOM's CookieContainer in src/cookie/CookieContainer.ts does not correctly validate or match Domain cookie attributes. It can accept a Domain unrelated to the origin setting the cookie, including a public suffix, and separately treats an unrelated suffix-sharing hostname as a match because cookieMatchesURL does not enforce a DNS-label boundary. In server-side rendering and prerendering applications that contact attacker-controlled origins and then make requests to a victim origin, these behaviors can plant and deliver a forged cookie, enabling cookie injection or session fixation. This issue is fixed in version 20.14.6.	6.5	More Deta
CVE-2026-62121	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Unlimited Elements Unlimited Elements For Elementor (Free Widgets, Addons, Templates) unlimited-elements-for-elementor allows PHP Local File Inclusion.This issue affects Unlimited Elements For Elementor (Free Widgets, Addons, Templates): from n/a through 2.0.26.	6.5	More Deta
CVE-2026-110292	The PayPlug for WooCommerce (Official) WordPress plugin before 3.1.1 does not verify that the requester owns the WooCommerce order named in a payment request, allowing unauthenticated users to disclose another customer's order key and cancel their unpaid guest order.	6.5	More Deta
CVE-2026-119200	Nuxt is an open-source web development framework for Vue.js. From 4.6.0 until 4.6.3, Nuxt resolves literal or percent-encoded dot segments before rendering a page while Nitro routing, server/middleware checks, and server route rules evaluate the unresolved path. A request such as /%2e/admin can therefore render app/pages/admin.vue and its server-rendered data while checks keyed to /admin, redirects, or per-route security headers do not apply. API handlers, appMiddleware, Nuxt 3, and Nuxt 4.0.0 through 4.5.x are not affected, and exploitation requires a client that sends dot segments without browser normalization. This issue is fixed in version 4.6.3.	6.5	More Deta
CVE-2026-59388	Cloud Controller (CAPI) leaks sensitive data into audit logs in multiple instances: custom buildpack credentials are exposed in audit events for app manifest application, creation, and updates; syslog drain URL credentials are exposed in user-provided service instance audit events; and service binding parameters are leaked in app manifest and service binding audit events.	6.5	More Deta
CVE-2026-119317	On Linux, an authenticated, low-privileged Nessus user with scan-creation rights could read arbitrary text files on the scanner host with the privileges of the nessusd process by running a custom Unix compliance audit against the scanner itself.	6.5	More Deta
CVE-2026-50541	Xibo is an open source digital signage platform with a web content management system and Windows display player software. Prior to 4.4.3, missing access-control checks on `GET /dataset/export/csv/{id}` allow an authenticated user to export data from any dataset, including datasets created by administrators, by iterating over `sequential dataset IDs`. Exploitation requires access to the privilege allowing edits, including deletion, to all created `DataSets` independently of Layouts. This privilege is not granted to non-administrators as standard. This issue is fixed in version 4.4.3.	6.5	More Deta
CVE-2026-119714	My Calendar WordPress plugin 3.8.8 before 3.8.11 contains a shortcode injection vulnerability that allows unauthenticated attackers to execute registered shortcodes via the mcs search parameter. The mcs value reaches mc_search_results() in src/my-calendar-search.php without bracket encoding before do_shortcode runs, so a GET request triggers shortcodes on any page or post, enabling content injection and spoofing.	6.5	More Deta
CVE-2026-119708	abp-next-admin 10.4.0 through 10.7.0 contains a cross-tenant authorization bypass in the BlobManagement download-by-name endpoint, letting authenticated users read other tenants' files. Attackers supply a victim tenantId in the request path, causing DownloadByNameAsync to switch tenant context and return blobs stored by that tenant.	6.5	More Deta
CVE-2026-118646	n8n before 1.123.85, 2.43.5, and 2.44.1 contains a regular expression denial of service vulnerability that allows authenticated members to block the event loop via crafted glob patterns. Attackers who can create and run workflows can submit a wildcard-heavy File(s) Selector pattern causing exponential backtracking, making the UI, API, webhooks, and health checks unresponsive until restart.	6.5	More Deta
CVE-2026-119702	WPGraphQL before 2.24.1 contains a missing authorization vulnerability in the createComment mutation that allows unauthenticated attackers to comment on non-public posts by bypassing post status checks. Attackers can attach comments to draft, private, trashed, or password-protected posts to leak hidden titles via moderator notifications, enumerate post IDs, and backdate comments or mark them as pingbacks.	6.5	More Deta
CVE-2026-67080	HCL BigFix AEX is affected by an Information Disclosure vulnerability due to improper handling of errors or exceptional conditions. This could allow an attacker to obtain sensitive technical information, including stack traces, system details, or internal paths, potentially facilitating further attacks.	6.5	More Deta
CVE-2026-110020	The Rich Showcase for Google Reviews plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 7.1.6 This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with contributor-level access and above, to retrieve the plugin's 127-character site-wide grw_auth_code authentication secret and use it to impersonate the WordPress site to the RichPlugins backend service at app.richplugins.com.	6.5	More Deta
CVE-2026-118685	ToolJet from 3.20.2-lts before 3.20.242-lts contains an authorization bypass in SignupDisableGuard, which treats the string signup setting 'false' as truthy, so instance-level signup restrictions are not enforced. Unauthenticated attackers can send POST requests to /api/signup without an organizationId to create an account, join the default workspace, and receive a valid session.	6.5	More Deta
CVE-2026-110691	The WPOrLogin WordPress plugin before 3.1.0 does not perform a capability check or validate a nonce before updating its hidden-login URL settings, which could allow unauthenticated attackers to reassign the login, registration and password-recovery slugs and lock the administrator out of the login interface.	6.5	More Deta
CVE-2026-118687	Coder before 2.29.21, 2.30.0 before 2.34.12, 2.35.0 before 2.35.9, 2.36.0 before 2.36.7, and 2.37.0 before 2.37.4 does not validate the audience claim of GCE instance-identity JWTs at the POST /api/v2/workspaceagents/google-instance-identity endpoint. Attackers who obtain an unexpired format=full identity token minted for another relying party can replay it to obtain that workspace agent's session token, which remains valid until the workspace's next build.	6.5	More Deta

CVE-2026-119369	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 6.18.2.	6.5	More Deta
CVE-2026-115415	Improper neutralization of input used for LLM prompting in the environment tool in Strands Agents Tools before 0.8.6 might allow remote actors to obtain the agent host's environment variables in cleartext, including cloud credentials and API keys, via a crafted prompt that disables the tool's secret masking. To remediate this issue, users should upgrade to version 0.8.6 or later and rotate any credentials that were present in the environment of agents that loaded the environment tool.	6.5	More Deta
CVE-2026-105457	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in HAVELSAN Inc. Liman MYS allows Path Traversal. This issue affects Liman MYS: before 2.3.5-1132.	6.5	More Deta
CVE-2026-62991	Shopper is a Headless e-commerce Admin Panel. Prior to 2.10.1, the customer detail route `/cpanel/customers/{user}/show` in `packages/admin/src/Livewire/Pages/Customers/Show.php` checks `read_customers` but looks up an arbitrary user ID without applying the `customers` role scope used by the listing. Authenticated staff holding `access_dashboard` and `read_customers` can change the user ID to retrieve administrator or staff profiles despite lacking `view_users`, which protects the separate team-management interface. The flaw exposes account profile data and permits user-ID enumeration through differing success, denial, and not-found responses. If the same role also holds `delete_customers`, `anonymizeAction()` operates on the unrestricted loaded user model and can enable destructive follow-up against non-customer accounts. This issue is fixed in version 2.10.1.	6.5	More Deta
CVE-2026-59386	A SpaceSupporter could improperly modify an application's start command and buildpack—actions requiring SpaceDeveloper privileges. This privilege escalation enables unauthorized retrieval of service credentials through malicious start commands or custom buildpacks.	6.5	More Deta
CVE-2026-86390	Dell PowerProtect Data Domain, Feature Release versions 7.7.1.0 through 8.8, LTS2024 release versions 7.13.1.0 through 7.13.1.80, LTS2025 release versions 8.3.1.0 through 8.3.1.40, LTS2026 release versions 8.6.1.0 through 8.6.1.20, contain a Missing Authorization vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Unauthorized access.	6.5	More Deta
CVE-2026-55369	Waline is a comment system with backend support. Prior to version 1.41.1, the login endpoint POST /api/token reads the email field from the request body without checking its type and passes it straight into the MongoDB storage query. When email is not a string (for example a JSON object such as {"$ne": null}), the MongoDB storage adapter's parseWhere silently DROPS the field rather than rejecting the request, producing an empty filter that matches ALL users. The endpoint then verifies the submitted password against the FIRST user returned (user[0]), which in Waline is the first-registered user — the site administrator. This is a PARTIAL authentication bypass, not a full one. The attacker still needs a valid password for that first user; this is not a zero-knowledge bypass and it does not disclose passwords. Its concrete effects are: (1) the email/identifier factor is removed for the administrator account, (2) user enumeration (a non-string email never fails the "no such user" branch), and (3) credential-stuffing amplification — an attacker can test a leaked or weak password against the administrator account without knowing the administrator's email. This issue has been patched in version 1.41.1.	6.5	More Deta
CVE-2026-54865	Subscriber Cross Site Scripting (XSS) in Podamibe Custom User Gravatar <= 1.0.8 versions.	6.5	More Deta
CVE-2026-115610	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PublishPress PublishPress Authors publishpress-authors allows Stored XSS.This issue affects PublishPress Authors: from n/a through 4.17.0.	6.5	More Deta
CVE-2026-18894	IBM Langflow OSS 1.0.0 through 1.12.4 could allow a remote attacker to trigger pre-existing stored Python component code in a public workflow, executing it under the flow owner's runtime context within the server process. This bypasses the intended trust boundary where public execution paths are restricted to server-trusted component code.	6.5	More Deta
CVE-2026-119365	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bPlugins Media Player Addons for Elementor – Media Player widget for WP media-player-addons-for-elementor allows Stored XSS.This issue affects Media Player Addons for Elementor – Media Player widget for WP: from n/a through 1.1.10.	6.5	More Deta
CVE-2026-48196	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Kaliforms Kali Forms kali-forms allows Stored XSS.This issue affects Kali Forms: from n/a through 2.4.27.	6.5	More Deta
CVE-2026-118097	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 2.14.0.	6.5	More Deta
CVE-2026-118095	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in David Lingren Media LIbrary Assistant media-library-assistant allows DOM-Based XSS.This issue affects Media LIbrary Assistant: from n/a through 3.42.	6.5	More Deta
CVE-2026-119328	Immich is a high-performance self-hosted photo and video management solution. Prior to 3.3.0, the unauthenticated machine-learning /predict endpoint in machine-learning/immich_ml/main.py accepted an options object and passed its values into model construction in machine-learning/immich_ml/models/base.py without restricting security-sensitive parameters. An attacker with network access to the service could set cache_dir to an arbitrary writable path, causing model downloads to write there and causing clear_cache() to pass that path to shutil.rmtree() after selected model-loading failures. Depending on filesystem permissions and the selected path, this could modify files in mounted data locations or recursively delete an attacker-selected directory. The model-name allowlist prevents this issue from becoming arbitrary-model deserialization or code execution. This issue is fixed in version 3.3.0.	6.5	More Deta
CVE-2026-116850	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in weDevs Happy Addons for Elementor happy-elementor-addons allows Stored XSS.This issue affects Happy Addons for Elementor: from n/a through 3.50.1.	6.5	More Deta
CVE-2026-118087	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Gemini Labs Site Reviews site-reviews allows Stored XSS.This issue affects Site Reviews: from n/a through 8.3.5.	6.5	More Deta
CVE-2026-116849	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bPlugins StreamCast streamcast allows Stored XSS.This issue affects StreamCast: from n/a through 2.4.6.	6.5	More Deta

CVE-2026-118094	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Igor Funa Ad Inserter ad-inserter allows Stored XSS.This issue affects Ad Inserter: from n/a through 2.8.18.	6.5	More Deta
CVE-2026-24533	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CozyThemes Cozy Blocks cozy-addons allows Stored XSS.This issue affects Cozy Blocks: from n/a through 2.2.27.	6.5	More Deta
CVE-2026-39735	Missing Authorization vulnerability in Crocoblock JetEngine jet-engine allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects JetEngine: from n/a through 3.9.0.1.	6.5	More Deta
CVE-2026-42703	Missing Authorization vulnerability in Kaliforms Kali Forms kali-forms allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Kali Forms: from n/a through 2.4.27.	6.5	More Deta
CVE-2026-119575	ArcadeDB from 26.8.1 before 26.10.2 contains a server-side request forgery vulnerability that allows authenticated users with updateDatabaseSettings to disable the LOAD CSV IP block list via ALTER DATABASE. Attackers can set arcadedb.opencypher.loadCsv.blockedIpRanges to an empty string, then issue LOAD CSV requests to read cloud metadata and internal loopback or private services.	6.5	More Deta
CVE-2026-39742	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Liquid Web / StellarWP Gutenberg Blocks by Kadence Blocks kadence-blocks allows Stored XSS.This issue affects Gutenberg Blocks by Kadence Blocks: from n/a through 3.8.0.2.	6.5	More Deta
CVE-2026-52709	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bPlugins Video Gallery Block video-gallery-block allows Stored XSS.This issue affects Video Gallery Block: from n/a through 1.6.0.	6.5	More Deta
CVE-2026-56056	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Mamunur Rashid The Post Grid the-post-grid allows Stored XSS.This issue affects The Post Grid: from n/a through 7.9.7.	6.5	More Deta
CVE-2026-55098	Arc is an open, SQL-native time-series database for telemetry. Prior to the repository-verified 26.06.2 repair, the remediation of `CVE-2026-47735` leaves a cross-database authorization bypass through DuckDB table-valued I/O functions. In `internal/database/sandbox.go`, `allowed_directories` uses `cfg.LocalStorageRoot`, configured by `storage.local_path`, while `enable_external_access=false` blocks access outside that entire multi-tenant root. `GetStoragePath` in `internal/storage/util.go` stores all databases beneath it. In `internal/api/query.go`, `extractTableReferences` skips names followed by an opening parenthesis and `checkQueryPermissions` allows queries with no extracted table references, including tokens with `permissions: []`. The `userSQLReadParquetPattern` denylist catches literal `read_parquet(` and the earlier protection also blocks `arc_partition_agg(`, but misses the `parquet_scan` alias and `glob`, `parquet_metadata`, `parquet_schema`, `read_blob`, `read_csv_auto`, `read_json` and `read_text`. A request to `POST /api/v1/query` using these unblocked functions passes `ValidateSQLRequest` and `convertSQLToStoragePaths` without tenant authorization, allowing reads and enumeration of other databases' time-series data, schema and per-column value-range statistics within the allowlisted root. The sandbox still blocks out-of-root OS files and HTTP SSRF, and the sibling SQLite token database outside the root is not exposed by this mechanism. The earlier 26.06.1 remediation does not comprehensively deny these I/O functions. Repository tag 26.06.2 contains the I/O-function repair and supplies the provisional remediation boundary; conflicting advisory affected-version statements require curator adjudication.	6.5	More Deta
CVE-2026-114706	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Chill Strong Testimonials strong-testimonials allows Stored XSS.This issue affects Strong Testimonials: from n/a through 3.3.15.	6.5	More Deta
CVE-2026-110881	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Brainstorm Force SureDash suredash allows Stored XSS.This issue affects SureDash: from n/a through 1.12.3.	6.5	More Deta
CVE-2026-107023	Insecure permissions in the ContentProvider component of mhss1 MyBrain v3.1.0 allows unauthorized attackers to arbitrarily read another user's private notes/tasks/diary content.	6.5	More Deta
CVE-2026-116857	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Crocoblock JetSmartFilters jet-smart-filters allows Stored XSS.This issue affects JetSmartFilters: from n/a through 3.8.6.2.	6.5	More Deta
CVE-2026-112348	Kirki plugin for WordPress before 6.2.5 contains a reCAPTCHA bypass vulnerability that allows unauthenticated attackers to submit frontend forms without valid verification by omitting the g-recaptcha-token field from POST requests to the form submission endpoint. Attackers can exploit the verify() method's early return on empty token values to submit unlimited forms, triggering notification emails, webhooks, and unbounded writes to the submissions table without completing reCAPTCHA validation.	6.5	More Deta
CVE-2026-54862	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Codection Import and export users and customers import-users-from-csv-with-meta allows Stored XSS.This issue affects Import and export users and customers: from n/a through 2.5.9.	6.5	More Deta
CVE-2026-117028	Skuul School Management System through version 2.6.5 is vulnerable to incorrect access control in the ResultChecker::checkResult method. An authenticated student can manipulate the studentId parameter to retrieve another student's examination results, including examination marks, without authorization.	6.5	More Deta
CVE-2026-39737	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Crocoblock JetElements For Elementor jet-elements allows Stored XSS.This issue affects JetElements For Elementor: from n/a through 2.9.2.6.	6.5	More Deta
CVE-2026-116252	pgAdmin 4's materialized view refresh passed the target database's name to psql's --dbname argument unchanged. libpq treats a --dbname value containing "=" (or a postgresql:// URI) as a full connection string, whose keywords override the host, port and other settings pgAdmin had supplied. A database whose name is such a string, which any role with CREATEDB can create, therefore redirected the psql process pgAdmin starts for the refresh to a host and port of the creator's choosing, and the connecting user's saved server password was presented to that endpoint. It also let the pgAdmin host be made to open connections to arbitrary addresses. The same weakness was fixed for Backup, Restore, Maintenance and Import/Export Data in earlier releases (CVE-2026-86862); the materialized view refresh was the remaining caller. The fix routes the name through the same database_conninfo() helper, so libpq treats it strictly as a database name. This issue affects pgAdmin 4: before 9.19.	6.5	More Deta

CVE-2026-119118	Crawl4AI before 0.9.5 contains an improper certificate validation vulnerability that allows network attackers to intercept crawls because Chromium always launches with --ignore-certificate-errors. Man-in-the-middle or DNS-controlling attackers can serve forged content to the crawler and read cookies and headers sent, while hard-coded --no-sandbox also overrides CRAWL4AI_CHROMIUM_SANDBOX.	6.5	More Deta
CVE-2026-110190	IBM Langflow OSS 1.0.0 through 1.12.4 could allow an authenticated user to traverse directories on the system. An attacker could send a specially crafted URL request to view arbitrary files on the system.	6.5	More Deta
CVE-2026-119551	Jellyfin through 12.4 contains an authorization bypass vulnerability in SuggestionsController.GetSuggestions that allows authenticated non-administrator users to bypass library and parental restrictions by omitting the userId parameter. Attackers can repeatedly call GET /Items/Suggestions without userId to enumerate restricted items, including IDs and server filesystem paths, and then stream them.	6.5	More Deta
CVE-2026-118084	Subscriber Insecure Direct Object References (IDOR) in Hotel Booking <= 3.8 versions.	6.5	More Deta
CVE-2026-119553	Moodle 5.3.0, 5.2.0 through 5.2.4, 5.1.0 through 5.1.8, 5.0.0 through 5.0.11, and through 4.5.15 contains a path traversal vulnerability in the Blackboard question import format. Teachers with question import or lesson edit rights can upload a crafted zip with img src values containing ../ sequences, copying server files like config.php into their draft area.	6.5	More Deta
CVE-2026-19610	A flaw was found in the platform-mbean component of JBoss EAP, which provides management access to JVM-level metrics and configurations. The issue occurs because the handler for the read-resource operation on the runtime management resource fails to perform required Role-Based Access Control (RBAC) checks. This allows an authenticated user with low-privileged access, such as the Monitor role, to view sensitive system properties and JVM configuration details that should be restricted.	6.5	More Deta
CVE-2026-88928	The PAYCOMET for WooCommerce WordPress plugin before 5.46 does not verify the cryptographic signature on its payment notification endpoint when the request references a tokenisation operation, allowing unauthenticated attackers to overwrite the stored payment token associated with existing orders and delete saved card records.	6.5	More Deta
CVE-2026-117548	A NULL pointer dereference flaw was found in 389-ds-base. This flaw occurs when a ModifyDN (rename) operation uses an attribute's schema alias name (such as "commonName") instead of its canonical name (such as "cn") as the new relative distinguished name. An authenticated attacker with the ModifyDN (rename) permission on the affected entry can use this flaw to crash the directory server, causing a denial of service.	6.5	More Deta
CVE-2026-116848	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in POSIMYTH Innovations The Plus Addons for Elementor Page Builder Lite the-plus-addons-for-elementor-page-builder allows Stored XSS.This issue affects The Plus Addons for Elementor Page Builder Lite: from n/a through 6.5.3.	6.5	More Deta
CVE-2026-119645	ZenTao PMS through 22.6 contains a missing authorization vulnerability in doc::ajaxGetDoc() that allows authenticated users to read documents without checkPrivDoc() access checks. Low-privilege attackers can enumerate sequential document ids to retrieve body and draft content of private documents and restricted library, product, project, or team documents.	6.5	More Deta
CVE-2026-110200	IBM Langflow OSS 1.0.0 through 1.12.4 could allow a remote authenticated attacker to obtain sensitive information due to cleartext storage of sensitive information.	6.5	More Deta
CVE-2026-110192	IBM Langflow OSS 1.0.0 through 1.12.8 could allow a remote authenticated attacker to obtain sensitive information due to insufficiently protected credentials.	6.5	More Deta
CVE-2026-119370	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 6.18.2.	6.5	More Deta
CVE-2026-116250	In server mode pgAdmin 4 validates a path a user gives for a file in their storage directory with check_access_permission() and then opened it by name. Several places opened it with a plain open() or handed the path to a utility that opened it later: the servers.json export and import and the import file listing, and the files given to pg_dump, pg_dumpall, pg_restore and psql by Backup, Restore and Import/Export Data. A symbolic link swapped in at the file or at any parent directory between the check and the open redirected the operation outside the storage directory, so a file could be written, overwritten or read, or loaded into a table, as the operating-system account running pgAdmin. A hard link to an outside file, which O_NOFOLLOW does not detect, and a FIFO, which could hang a request, had the same effect. CVE-2026-86861 fixed this for the File Manager's save_file; these were the remaining paths. Exploitation requires creating such a link or FIFO inside the user's storage directory. pgAdmin offers no way to do so, and the per-user storage directories belong to the pgAdmin account, so this requires write access to the storage backend as a different operating-system user, for example a shared or network-mounted storage directory, and winning the race. The fix opens each file by walking down from the storage directory one component at a time with O_NOFOLLOW, accepting only a regular file with one link, and passes the utilities the open descriptor (/dev/fd/N) on Linux. Error messages no longer include the server path. This issue affects pgAdmin 4: before 9.19.	6.5	More Deta
CVE-2026-55493	HotCRP is conference review software. Starting with 2.101, the `cmt:` search term checks whether a comment is visible to the searching user but fails to check whether the commenter's identity should be visible. A `cmt:USER` search can therefore match a paper with a visible comment authored by USER even when the comment is supposed to be anonymous. An authenticated user with access to the search can infer the author of an anonymous comment, compromising reviewer anonymity. Comments that the user cannot see remain excluded from search results. The advisory prose identifies 3.3 as fixed, its affected-version metadata excludes 3.3, and the verified repository tag 3.3 already contains the identity-check fix; however, its patched-version metadata instead lists 3.3.1. This fixed-version source conflict remains unresolved.	6.5	More Deta
CVE-2026-118192	The JoomSport – for Sports: Team & League, Football, Hockey & more plugin for WordPress is vulnerable to generic SQL Injection via the 'team_id' parameter in all versions up to, and including, 5.7.11 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. The vulnerable code path is reached when the season has no associated joomsport_tournament term, which is the default state for newly created seasons.	6.5	More Deta
CVE-2026-107035	Insecure permissions in the object/Page.java component of MBasov OMN Outline notes Markdown versionCode 3400 allows unauthorized attackers to arbitrarily write content into another user's private storage via a crafted payload.	6.5	More Deta
CVE-2026-107033	Insecure permissions in the MirakelInternalContentProvider component of Mirakel v3.0 (versionCode 60) allows unauthorized attackers to arbitrarily read and modify another user's task database.	6.5	More Deta
CVE-			

2026-104316	IBM Langflow OSS 1.0.0 through 1.12.3 could allow an authenticated attacker to cancel any victim's running background workflow job by sending a single HTTP request, resulting in loss of in-progress compute work with no flow-level permission check.	6.5	More Deta
CVE-2026-104314	IBM Langflow OSS 1.0.0 through 1.12.3 could allow an authenticated attacker with a read or share grant on a target flow to retrieve the flow owner's stored third-party credentials in cleartext from the API response.	6.5	More Deta
CVE-2026-104309	IBM Langflow OSS 1.0.0 through 1.12.3 could allow a remote authenticated attacker to obtain sensitive information due to improper limitation of a pathname to a restricted directory.	6.5	More Deta
CVE-2026-116240	In server mode pgAdmin 4 validates a path into the user's storage directory with check_access_permission(), which builds the absolute path with get_abs_path(). Several callers then acted on a path they built differently, so the path checked and the path used could name different files: - Opening a file in the Query Tool, the Google client secret and, on Windows, Import/Export Data, Backup, Restore and saving a file joined the path to the storage directory after stripping leading slashes and backslashes. On POSIX a path checked as a name inside storage could become an absolute path once stripped, so any file the pgAdmin account can read could be opened; on Windows a path naming a drive discarded the storage directory, so these could read, or write, outside it. - Listing a folder decoded the path a second time after the check, so a folder named like an encoded "..", which a user can create, listed any directory on the host. - Download, delete, rename and the file-exists check appended the path to the storage directory without a separator, so in a deployment where one user's storage directory name is a prefix of another's, another user's files could be read, deleted or moved; download also checked the path appended to itself. - Creating a folder could create one in another user's directory. The fix makes check_access_permission() return the path it checked and every caller act on that path, decodes folder paths once, and opens, deletes and renames files relative to directories opened from the storage directory without following symbolic links. Desktop mode is not affected. This issue affects pgAdmin 4: before 9.19.	6.5	More Deta
CVE-2026-116246	To pass a server's password to psql and to the utilities pgAdmin 4 runs as background processes, the server manager wrote it into pgAdmin's own process environment: as PGPASSWORD for the PSQL tool, and under a per-process variable for a utility. Nothing removed it afterwards. pgAdmin's environment is shared by every user's requests and copied into every process it starts, so in server mode another user's later PSQL session or utility inherited the password, and libpq used PGPASSWORD for any connection made without a password of its own, letting one user connect with another user's saved password. The fix puts the password only into the environment built for the process that needs it and starts psql with a copy of pgAdmin's environment instead of the environment itself. This issue affects pgAdmin 4: before 9.19.	6.5	More Deta
CVE-2026-109822	Yamaha wireless LAN router NWR100 provided by Yamaha Corporation contains an issue with insecure storage of sensitive information. Configuration files generated by the CONFIG file export function may be read by an unauthenticated attacker.	6.5	More Deta
CVE-2026-119300	Wekan is open source kanban built with Meteor. Prior to 11.11, the user-search publication in server/publications/users.js and the searchUsers method in server/models/users.js pass authenticated user-controlled searchTerm and query values to new RegExp() without escaping regular-expression metacharacters. MongoDB-backed deployments evaluate the resulting patterns with PCRE2, allowing a logged-in user to submit catastrophic-backtracking expressions that consume database CPU and degrade or deny service to other users; searchUsers additionally requires board membership or site-admin status. The FerretDB v1 / RE2 unaffected configuration is not practically affected by catastrophic backtracking. This issue is fixed in version 11.11.	6.5	More Deta
CVE-2014-125137	C97net qEngine CMS through 6.0.0, Kemana Directory through 1.5.6, and Cart Engine through 3.0.0 contain a local file inclusion vulnerability in the run parameter of admin/task.php. Authenticated administrators can supply directory traversal sequences in the run parameter to include and disclose local files readable by the web server.	6.5	More Deta
CVE-2026-48195	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bPlugins PDF Poster pdf-poster allows Stored XSS.This issue affects PDF Poster: from n/a through 2.6.1.	6.5	More Deta
CVE-2026-110181	PostgreSQL Anonymizer contains a vulnerability related to anonymization functions defined using SQL-standard function bodies. PostgreSQL analyses such functions at declaration time, while Anonymizer only attempts to check them at execution time. This problem can be exploited by any user with the TEMPORARY privilege. The issue is fixed in PostgreSQL Anonymizer 3.3.0 and later versions.	6.5	More Deta
CVE-2026-50539	Xibo is an open source digital signage platform with a web content management system and Windows display player software. Prior to 4.4.3, missing object-level authorization on `/notification/export/{id}` allows an authenticated user to download attachments from any notification, including notifications created by administrators, by iterating over `sequential notification IDs`. Exploitation requires access to the `Notification Centre` to view past notifications, a privilege granted to non-administrators as standard. This issue is fixed in version 4.4.3.	6.5	More Deta
CVE-2026-116853	Unauthenticated Broken Access Control in GiveWP <= 4.19.0.1 versions.	6.5	More Deta
CVE-2026-105617	PostgreSQL Anonymizer doesn't invalidate plans prepared after a rule was added or a role changed. Users using such plans can still see the unmasked data until the end of the session. The problem is resolved in PostgreSQL Anonymizer 3.3.0 and later versions.	6.5	More Deta
CVE-2026-116854	Subscriber Cross Site Scripting (XSS) in WP Customer Area <= 8.4.0 versions.	6.5	More Deta
CVE-2026-91920	A flaw was found in the ChunkReader component of the Undertow web server, which is used to handle chunked transfer encoding in HTTP requests. The issue occurs because a security check for the chunk size is performed before the value is shifted, allowing a specifically crafted 15-digit chunk size to bypass the limit and overflow into internal state flags. This can cause the server to terminate a request body prematurely and interpret the remaining data as a separate, smuggled request.	6.5	More Deta
CVE-2026-105620	PostgreSQL Anonymizer doesn't mask data returned by a sub-query in a rule. The problem is resolved in PostgreSQL Anonymizer 3.3.0 and later versions.	6.5	More Deta
CVE-2026-62277	LubeLogger is a self-hosted, open-source, web-based vehicle maintenance and fuel mileage tracker. Prior to 1.6.8, `PrintRecordStickers` in `/Controllers/VehicleController.cs` checks through `CollaboratorFilter` that the authenticated caller can view the supplied `vehicleId`, but fetches caller-supplied `recordIds` without checking that each record's `VehicleId` belongs to the authorized vehicle. An authenticated user can submit `POST /Vehicle/PrintRecordStickers` with an authorized `vehicleId`, enumerate other users' integer record IDs and select an `ImportMode` to retrieve records across the service, gas, repair, upgrade, tax, supply, note, odometer, reminder, plan, inspection and equipment stores. Returned information includes descriptions, costs, notes, mileage, extra fields and file attachment metadata, allowing cross-user disclosure of vehicle maintenance records. This issue is fixed in version 1.6.8.	6.5	More Deta

CVE-2026-114711	Subscriber Cross Site Scripting (XSS) in MultiVendorX <= 5.0.20 versions.	6.5	More Deta
CVE-2026-115455	A flaw was found in GCC libstdc++. When an application extracts data into a bitset from a wide-character stream, internal stack memory allocation fails to properly account for character size and alignment. An attacker capable of supplying crafted input to an affected application could trigger a stack-based buffer overflow leading denial of service (DoS).	6.5	More Deta
CVE-2026-5461	The Forminator Forms plugin for WordPress is vulnerable to Limited File Deletion in all versions up to, and including, 1.55.0.2. This is due to the plugin accepting arbitrary upload field metadata from POST requests in draft submissions without proper validation, which is then used to delete files when a subsequent draft references the poisoned draft via the previous_draft_id parameter. This makes it possible for unauthenticated attackers to delete arbitrary non-PHP files within the wp-content/uploads/ directory.	6.5	More Deta
CVE-2026-116609	The WP Visitor Statistics (Real Time Traffic) plugin for WordPress is vulnerable to SQL Injection via the 'from' (and sibling 'to'/'first'/'second') shortcode attribute of the [wsm_showTrafficStatsList] shortcode in versions up to, and including, 8.8 This is due to insufficient escaping on the user-supplied attribute and lack of sufficient preparation on the existing SQL query: `shortcode_atts()` returns attacker-supplied shortcode attributes verbatim (WP core performs no sanitization), only `$atts['id']` is re-sanitized afterward, and the raw value is then concatenated into a double-quoted SQL string literal inside `fnGetHourlyReportByDateNameTimeZone()` (`includes/wsm_db.php:1449`) and executed via `$wpdb->get_results()`. This makes it possible for authenticated attackers, with Contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	6.5	More Deta
CVE-2026-116750	The VikRentCar Car Rental Management System plugin for WordPress is vulnerable to blind SQL Injection via the 'catid' parameter in all versions up to, and including, 1.4.10 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. A Contributor-level user can store a malicious block via the REST API in a pending post and trigger server-side rendering by previewing that post, bypassing wp_magic_quotes since the attribute is sourced from post_content via parse_blocks rather than a superglobal.	6.5	More Deta
CVE-2026-102905	The The Ad Inserter – Ad Manager & AdSense Ads plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 2.8.19 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 an administrator to have configured an ad block containing a dynamic tag such as {title}, {tag}, {category}, or {smart-tag} with display enabled on search pages, which is a normal and documented plugin configuration.	6.5	More Deta
CVE-2026-120007	NodeBB 1.18.0 through 4.16.5 contains an authorization bypass vulnerability that allows unauthenticated visitors to act on other accounts by supplying a uid during POST /register. Attackers can submit an empty email at the /register/complete interstitial to clear a victim's email and confirmation state and revoke all their sessions.	6.5	More Deta
CVE-2026-115947	Unauthenticated Sensitive Data Exposure in HUSKY <= 1.4.6 versions.	6.5	More Deta
CVE-2026-118194	The Page and Post Restriction plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 1.6.1 This is due to the `papr_restrict_page_post_rest_api()` function, hooked on `rest_pre_dispatch`, re-authenticating the current user from the `wordpress_logged_in` cookie via `wp_set_current_user()` for any GET or HEAD REST request where the current user is 0, without verifying a REST nonce — silently undoing the nonce-zeroing that WordPress core's `rest_cookie_check_errors()` performs on cookie-authenticated requests that lack an `X-WP-Nonce` header or `_wpnonce` parameter. Combined with WordPress's permissive REST CORS behavior — which echoes the request `Origin` and sets `Access-Control-Allow-Credentials: true` — this allows an unauthenticated attacker to read REST API GET responses as a logged-in victim, exposing role-restricted and private post/page content, victim user profile data via `/wp-json/wp/v2/users/me`, and comments the victim is authorized to see. This requires the attacker to lure a logged-in user into visiting an attacker-controlled page that issues credentialed cross-origin `fetch` requests against the target site's REST API; no nonce or further victim interaction beyond the page visit is needed.	6.5	More Deta
CVE-2026-76024	Use after free in MediaStream in Google Chrome prior to 156.0.8078.79 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: Critical)	6.5	More Deta
CVE-2026-107257	Incorrect Authorization vulnerability in Drupal Actstream allows Forceful Browsing. This issue affects Actstream versions: from 0.0.0 to 2.0.1, from 2.1.0 to 2.1.1.	6.5	More Deta
CVE-2026-119086	Missing queue-set type validation in the queue-set selection system call in FreeRTOS-Kernel before V11.3.3 on MPU-enabled ports with queue sets enabled allows a local unprivileged task to write actor-controlled data beyond a pointer-sized object on the privileged kernel stack, affecting privileged memory across the MPU isolation boundary. To remediate this issue, users should upgrade to FreeRTOS-Kernel V11.3.3, rebuild, and reflash affected firmware. Builds that do not enable queue sets are not affected.	6.5	More Deta
CVE-2026-54850	Subscriber Broken Access Control in Booking and Rental Manager <= 2.8.2 versions.	6.5	More Deta
CVE-2026-118581	A BSON encoding component of the MongoDB Java Driver does not verify that an externally supplied raw document's self-declared length agrees with the extent of the byte range it is given before that range is copied into an outgoing database command. An application that wraps untrusted raw bytes in such a document and uses it as part of a command can therefore emit a structurally inconsistent message, causing the database to interpret attacker-supplied trailing content as additional fields of the surrounding command. No authentication to the driver or database is required beyond the ability to influence those bytes through the victim application, and no user interaction is needed. The result is unintended modification of the command actually executed, which can alter the data read or written under the application's credentials.	6.5	More Deta
CVE-2026-118635	The The GeoDirectory – WP Business Directory Plugin and Classified Listings Directory plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 2.8.198 This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes.	6.5	More Deta
CVE-2026-13747	The Meow Gallery plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 5.5.4 This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with author-level access and above, to enumerate and read metadata — including post ID, title, date, author, and status — of all private and draft posts on the site, including those authored by other users.	6.5	More Deta
	The Majestic Support – The Leading-Edge Help Desk & Customer Support Plugin plugin for WordPress is vulnerable to generic SQL Injection via the		

CVE-2026-115820	'columns (array keys)' parameter in all versions up to, and including, 1.2.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for 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. Any authenticated WordPress user with Subscriber-level access can exploit this because the 'saveusereraserequest' task is whitelisted for front-end customer use, the plugin auto-provisions a help-desk record for every WordPress account, and the only guard is a nonce the attacker legitimately obtains from their own 'Add erase request' page.	6.5	More Deta
CVE-2026-82962	ethernet_fill_header() in subsys/net/l2/ethernet/ethernet.c can prepend the Ethernet header in place, by pushing it into the headroom of the packet's first fragment, instead of allocating a separate header fragment. Before this fix the in-place path was selected purely from the build-time value of CONFIG_NET_L2_ETHERNET_RESERVE_HEADER, with no check that the packet actually has that headroom, and then called net_buf_push(pkt->buffer, hdr_len). Only Ethernet TX allocations reserve that space: net_pkt_alloc_buffer() invokes the L2 alloc hook (ethernet_l2_alloc()) only when is_pkt_tx() is true and the packet's interface is the Ethernet interface. A packet that was allocated by a different L2 and then handed to Ethernet for transmission therefore has too little (usually zero) headroom. Such packets are produced by ordinary routing and tunnelling paths: net_route_packet_if() re-targets a received packet to another interface when CONFIG_NET_IPV4_FORWARDING / CONFIG_NET_IPV6_FORWARDING are enabled (for example an 802.15.4/OpenThread or PPP interface forwarding to Wi-Fi/Ethernet), net_route_ipv6_mcast_forward_packet() forwards an RX-slab clone that carries no reserve, and the IPIP tunnel interface_send() prepends an outer IP header allocated on the virtual interface. In these configurations a remote or adjacent attacker triggers the condition simply by sending traffic that the device forwards. Because net_buf_simple_push() only asserts on the headroom bound, a build without CONFIG_ASSERT (and without the newer CONFIG_NET_BUF_HARDENING) moves the fragment data pointer below the start of its data block and writes 14 bytes — 18 with VLAN — of Ethernet header out of bounds. With the default fixed-size buffer pools this overwrites the tail of the neighbouring buffer's payload or memory preceding the pool array; with variable-size pools it overwrites the buffer reference count and the heap chunk header. The attacker controls neither the written bytes nor the offset, so the practical impact is memory corruption leading to a crash, packet corruption, or heap inconsistency rather than controlled code execution. The fix takes the in-place path only when net_buf_headroom(pkt->buffer) is large enough and otherwise falls back to a separate header fragment.	6.5	More Deta
CVE-2026-27061	Subscriber Cross Site Scripting (XSS) in User Registration <= 5.3.0 versions.	6.5	More Deta
CVE-2026-118698	The JoomSport – for Sports: Team & League, Football, Hockey & more plugin for WordPress is vulnerable to generic SQL Injection via the 'pgroup' parameter in all versions up to, and including, 5.7.14 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. A Contributor-level user can trigger the vulnerable code path by authoring a post containing the [jsMatchPlayerList] shortcode with a malicious pgroup value and previewing it, as WordPress allows shortcode execution during post preview for the post's author.	6.5	More Deta
CVE-2026-88858	A user with the Viewer role in Grafana can crash the server by submitting a crafted server-side math expression (uncontrolled recursion). A user with permission to provision alert rules can make the outage persist across restarts.	6.5	More Deta
CVE-2026-39739	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Brainstorm Force Ultimate Addons for Elementor - Lite header-footer-elementor allows Stored XSS.This issue affects Ultimate Addons for Elementor - Lite: from n/a through 2.9.5.	6.5	More Deta
CVE-2026-118952	A flaw was found in the Kroxylicious ACL authorizer. Its prefix-matching logic may apply a rule to a principal of a different type, or fail to check a broader matching rule when prefixes overlap. Depending on the ACL configuration, this may allow an authenticated Kafka client to access a resource (such as read a topic) that should be denied.	6.5	More Deta
CVE-2026-117615	Jenkins 2.587 and earlier, LTS 2.580.1 and earlier follows symbolic links when copying the directory of an item being renamed, allowing attackers with Item/Create and Item/Configure permission to read arbitrary files on the Jenkins controller file system.	6.5	More Deta
CVE-2026-107251	Incorrect Authorization vulnerability in Drupal Entity Reference Manager (Merge entities) allows Forceful Browsing. This issue affects Entity Reference Manager (Merge entities) versions: from 0.0.0 to 1.0.3.	6.5	More Deta
CVE-2026-119842	A flaw was found in GStreamer's gst-plugins-base MicroDVD subtitle parser. When processing a specially crafted subtitle file, the parser may dereference a NULL pointer, causing the application to crash when a user opens or plays media with a malformed MicroDVD (.sub) subtitle file.	6.5	More Deta
CVE-2026-116410	Unauthenticated Arbitrary Content Deletion in Masteriyo - LMS <= 3.4.3 versions.	6.5	More Deta
CVE-2026-76005	The WP Inventory Manager plugin for WordPress is vulnerable to time-based SQL Injection via 'sort_order' Shortcode Attribute in all versions up to, and including, 2.5.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. This can be exploited by a Contributor via the [wpinventory_categories] shortcode embedded in a draft post rendered through preview, without requiring the post to be published.	6.5	More Deta
CVE-2026-119117	Insertion of sensitive information into a log file in Amazon Kinesis Producer Library for Java before 1.0.8, when the library's logger is configured at DEBUG log level, might allow local users to obtain the AWS credentials that the library resolved for the application. Separately, affected versions of the library pass these credentials to the native child process as command-line arguments, where a local user can read them from the process argument list. To remediate this issue, users should upgrade to version 1.0.8 or later, rotate any long-term IAM user keys, revoke active role sessions where needed, and restrict or redact log data written by an affected version. 0.x users should migrate to software.amazon.kinesis:amazon-kinesis-producer 1.0.8 or later.	6.5	More Deta
CVE-2026-119727	A flaw was found in GStreamer's gst-plugins-bad H.265 video parser. When parsing a specially crafted H.265 bitstream containing a Screen Content Coding (SCC) extension with certain palette predictor initializer settings, an integer underflow in the upper-bound computation allows the parser to accept an out-of-range value for the number of palette predictor entries. This causes the parser to write beyond the end of a fixed-size array, resulting in memory corruption and an application crash. Successful exploitation requires an attacker to provide a malformed H.265 media file to a vulnerable application, and is limited to a denial-of-service impact.	6.5	More Deta
CVE-2026-119729	A flaw was found in GStreamer. An integer overflow vulnerability in the AV1 LEB128 variable-length integer parser allows a remote attacker to cause a crash in applications that process AV1 media content. By crafting a malformed AV1 bitstream containing an invalid LEB128-encoded value, an attacker can cause integer overflow in the parser, resulting in incorrect length values being used during stream processing, which can lead to a denial of service.	6.5	More Deta

CVE-2026-119728	A flaw was found in the H.264 video parser in gst-plugins-bad. When processing a specially crafted H.264 video file with malformed Multiview (MVC) Sequence Parameter Set data, the parser can dereference a NULL pointer during the cleanup of partially allocated internal structures after a parse failure. This can cause the application using GStreamer to crash, resulting in a denial of service.	6.5	More Deta
CVE-2026-96389	Missing Authorization vulnerability in Drupal Xray Audit allows Forceful Browsing. This issue affects Xray Audit versions: from 0.0.0 to 1.6.3, from 2.0.0 to 2.0.4, from 3.0.0 to 3.1.1.	6.5	More Deta
CVE-2026-118539	Missing Authorization vulnerability in Drupal Commerce Core allows Forceful Browsing. This issue affects Commerce Core versions: from 0.0.0 to 2.41, from 3.0.0 to 3.3.13.	6.5	More Deta
CVE-2026-55551	ZAC is an open-source, workflow-based Common Ground component for Dutch municipal case management. Prior to 5.2.0, by-id read endpoints in `src/main/kotlin/nl/info/zac/app/zaak/ZaakRestService.kt` omit `assertPolicy`(`policyService.readZaakRechten(zaak).lezen`) authorization. `RequestAuthorizationFilter` and `hasAnyApplicationRole` require only an application role on any zaaktype, not the target case's type, while `zaak-rechten.rego` enforces the actual `zaaktype_allowed` boundary only when invoked. An authenticated low-privileged municipal user who knows a case or decision UUID can use `GET /rest/zaken/besluit/zaakUuid/{uuid}` (`listBesluitenForZaakUUID`) to read decisions including types, dates, and free-text toelichting; `GET /rest/zaken/besluit/{uuid}/historie` (`listBesluitHistorie`) to read audit old/new values; and `GET /rest/zaken/{uuid}/process-diagram` (`downloadProcessDiagram`) to read BPMN workflow state across unauthorized zaaktypes. The advisory also identifies `zaak/{uuid}/afzender` (`listAfzendersVoorZaak`) as exposing zaaktype mailbox configuration without a policy check. The search/_zoek path is correctly authorization-filtered and is not part of this by-id read cluster. This issue is fixed in version 5.2.0.	6.5	More Deta
CVE-2026-9239	The Meow Gallery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Attachment Alt Text (aria-label attribute) in all versions up to, and including, 5.5.1 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. The vulnerable code path is only reachable when a gallery item is rendered as a link (i.e., link_href is non-empty), and exploitation relies on the fact that WordPress's sanitize_text_field() strips angle-bracketed tags but preserves double quotes, allowing an attacker to break out of the aria-label attribute context and inject event-handler attributes such as onclick.	6.4	More Deta
CVE-2026-77188	The Waitlist Woocommerce (Back in stock notifier) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'type' Shortcode Attribute in all versions up to, and including, 2.9.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The wp_kses_post filter applied on contributor post save does not prevent this vulnerability because shortcode attribute values are not HTML and pass through kses unchanged; the payload is materialized only at render time when the shortcode is expanded.	6.4	More Deta
CVE-2026-118634	The Events Made Easy plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'width' parameter in all versions up to, and including, 3.3.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Deta
CVE-2026-104740	The If-So Dynamic Content – Elementor & All Page Builders Personalization plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'conversion' Shortcode Attribute in all versions up to, and including, 1.10.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Deta
CVE-2026-110071	The Mang Board plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'align' parameter in all versions up to, and including, 2.4.5 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. Because the payload contains no angle brackets, wp_kses_post leaves the shortcode intact on save, allowing the malicious attribute value to survive post submission and fire in any viewer's browser — including an administrator previewing a pending post.	6.4	More Deta
CVE-2026-109590	The Tour Booking Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'width', 'height' and 'zoom' shortcode attributes of the [ttbm-hotel-map] shortcode in versions up to, and including, 2.3.6 This is due to insufficient input sanitization and output escaping on user supplied attributes in the ttbm_hotel_map_shortcode() function, which concatenates the raw attribute values into double-quoted HTML attributes of an <iframe> tag. 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 Deta
CVE-2026-109978	The Cozy Blocks – Website Builder for WordPress Block Editor | Gutenberg Blocks, Patterns & Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'productRating.iconColor' parameter in all versions up to, and including, 2.2.27 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 vulnerable code path is only reached when the productRating option is enabled and the associated WooCommerce product has a non-zero rating.	6.4	More Deta
CVE-2026-107625	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 'user_url' parameter in all versions up to, and including, 2.14.0 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. Successful exploitation requires a visitor to click the attacker's Website URL link on their public Ultimate Member profile, a condition that is trivially met since the redirect-confirmation onclick handler is enabled by default on all new installations.	6.4	More Deta
CVE-2026-104729	The Avada (Fusion) Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'tab_index, empty_notice' parameter in all versions up to, and including, 3.16.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. wp_kses_post does not strip the payload on save because the dangerous characters reside within shortcode attribute text between square brackets, which kses treats as plain text rather than HTML markup.	6.4	More Deta
CVE-2026-118500	The Cool FormKit Lite – Advanced Form Builder for Elementor plugin for WordPress is vulnerable to Stored DOM-Based Cross-Site Scripting via the '_elementor_data.form_fields[].custom_id' parameter in all versions up to, and including, 2.7.9 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. The esc_html() call applied at server emission is bypassed because the HTML fragment-serialization algorithm restores " to a raw double-quote inside text nodes when jQuery .html() extracts the template, allowing the attacker-controlled custom_id to break out of an HTML attribute context within the plugin's own frontend script.	6.4	More Deta
CVE-2026-103996	The If-So Dynamic Content – Elementor & All Page Builders Personalization plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'url' parameter in all versions up to, and including, 1.10.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The injected script executes specifically in the administrator's browser session, as the vulnerable branch only renders	6.4	More Deta

	when an administrator previews or opens the post containing the crafted shortcode.		
CVE-2026-109972	The s2Member – Excellent for All Kinds of Memberships, Content Restriction Paywalls & Member Access Subscriptions plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'date_format' parameter in all versions up to, and including, <= 261011 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() on save because it contains no literal angle brackets — only backslash-escaped sequences that PHP's date() materializes into HTML tag characters at render time after WordPress's shortcode_parse_atts() applies stripcslashes() to the attribute value.	6.4	More Deta
CVE-2026-115711	Insertion of Sensitive Information into Externally-Accessible File or Directory (CWE-538) in Elastic Cloud Enterprise (ECE) can lead to credential disclosure via Retrieve Embedded Sensitive Data (CAPEC-37). ECE stores runtime information about platform service containers in a location that lower-privileged platform components can read, and this information includes secrets from the container configuration. An attacker with access to the internal ECE platform services can obtain these secrets, which include role tokens. A role token can let the attacker add an unauthorized host to the installation with the roles of that token.	6.4	More Deta
CVE-2026-110533	The FV Flowplayer Video Player plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'fv_player_videos[_fv_player_user_video][]' parameter in all versions up to, and including, 7.5.55.7212 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This requires an administrator to have enabled the "Allow visitors to upload videos to their profile" (profile_videos_enable_bio) setting before Subscriber-level users can submit profile videos.	6.4	More Deta
CVE-2026-109385	The UiChemy – Convert Figma, Prompts and AI Builds to Elementor, Gutenberg and Bricks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'actions[save_builder][data][elements][...][settings][slot_{N}_link][url]' parameter in all versions up to, and including, 5.3.0 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. The injected javascript: payload fires on click rather than on page load, making exploitation contingent on a privileged user such as an Editor or Administrator clicking the attacker-crafted link while reviewing or previewing the Contributor's post.	6.4	More Deta
CVE-2026-109891	Missing Authorization vulnerability in weDevs Happy Addons for Elementor happy-elementor-addons allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Happy Addons for Elementor: from n/a through 3.50.1.	6.4	More Deta
CVE-2026-109370	The Document Embedder – let visitors read files without downloading plugin for WordPress is vulnerable to Stored DOM-Based Cross-Site Scripting via the 'content (post_content containing block JSON documentSource.doc)' parameter in all versions up to, and including, 2.4.0 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. The payload is triggered specifically when the victim clicks the embedded document's Download button, which causes the de_track_download AJAX fallback path to programmatically create an anchor with the attacker-controlled href and call .click() — a condition reached because supplying docId=0 causes can_read_document() to return false, bypassing the normal download flow.	6.4	More Deta
CVE-2026-115869	The Themify Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'variations' repeater field of Custom Font (tb_cf) posts in versions up to, and including, 7.8.4. This is due to insufficient input sanitization and output escaping on the variations post meta: Themify_Metabox::_save_meta() only passes the value through wp_kses_data() when the field type is 'textbox' or 'textarea', so the 'repeater' field writes attacker-controlled sub-fields (style, woff/woff2/ttf/svg/eot URLs) to update_post_meta() verbatim, and Themify_Custom_Fonts::render_columns() later echoes those values unescaped inside a <style> block on the Custom Fonts admin listing. 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 (specifically, the Custom Fonts admin listing).	6.4	More Deta
CVE-2026-109215	The LiteSpeed Cache plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'bbp_reply_content' parameter in all versions up to, and including, 7.9.1 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. Exploitation requires that an administrator has enabled Viewport Images (VPI) and configured a VPI filename that matches an image the attacker can embed in user-generated content — such as a bbPress topic where Subscriber-level Participants are permitted to post replies containing raw img tags.	6.4	More Deta
CVE-2026-104727	The Sequential Order Numbers for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'condition' Post Meta Array Keys in all versions up to, and including, 3.6.5 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 Deta
CVE-2026-107710	The Hustle – Email Marketing, Lead Generation, Optins, Popups plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'content[title]' parameter in all versions up to, and including, 7.8.14.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with custom-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Exploitation requires that an administrator has explicitly granted the 'Create and Update Modules' (hustle_create / hustle_edit_module) capability to the attacker's role via the plugin's own Settings → Permissions feature; this delegation is not enabled by default.	6.4	More Deta
CVE-2026-108366	The easy.jobs – AI powered Job Listing, Job Board, Career Page, Recruitment & Hiring Solution plugin for WordPress is vulnerable to Authenticated (Contributor+) Stored Cross-Site Scripting via the 'icon' attribute of the easyjobs/job-list Gutenberg block in all versions up to, and including, 2.8.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Deta
CVE-2026-109209	The All-in-One Video Gallery – Video Player & Galleries for YouTube, Vimeo & Self-Hosted Videos plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'custom_fields[embedcode]' parameter in all versions up to, and including, 4.9.7 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 sanitization bypass is possible because the save_meta_data() handler returns early when $_POST['post_type'] is absent — a condition always true during XML-RPC requests — and the plugin unconditionally grants Subscribers the publish_aiovg_videos capability, making this exploitable by any authenticated user via a single wp.newPost XML-RPC call.	6.4	More Deta
CVE-2026-93293	The Password Protected plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the bundled Freemius SDK's purchase-completion handler in all versions up to, and including, 2.8.4 due to insufficient input sanitization and output escaping. Once the site's Freemius opt-in is complete (the normal state after an administrator clicks "Allow & Continue"), the handler processes the 'purchased_plan' request parameter on any wp-admin request from an authenticated user without any capability, nonce, or purchase validation, and stores it in a persistent, site-wide administrative notice. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts that execute automatically when an administrator views a standard admin page such as their Profile page.	6.4	More Deta
	The GeoDirectory – WP Business Directory Plugin and Classified Listings Directory plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the listing description (post_content) in versions up to, and including, 2.8.199 This is due to insufficient input sanitization on save (the bundled		

CVE-2026-119113	geodir_kses_safe_embed_attributes() helper only neutralises data-embed-url, data-src and data-embed, while WordPress core wp_kses_post permits data-* attributes on standard HTML tags) combined with the AyeCode UI library initializing every [data-bs-toggle="popover-html"] element with { html: true, sanitize: false }, which inserts the attacker-controlled data-bs-content value into the popover body as HTML at render time. 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 Deta
CVE-2026-119176	The CP Multi View Events Calendar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Subject' parameter in all versions up to, and including, 1.4.43 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 required nonce is localized to any published page carrying the calendar shortcode, making the adddetails endpoint reachable by any authenticated user with Subscriber-level access or above.	6.4	More Deta
CVE-2026-109974	The All-in-One Video Gallery – Video Player & Galleries for YouTube, Vimeo & Self-Hosted Videos plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'more_link' parameter in all versions up to, and including, 4.9.7 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 Deta
CVE-2026-77871	The Post Snippets – Custom WordPress Code Snippets Customizer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Shortcode Attributes in all versions up to, and including, 4.2.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Entity-encoded payloads such as <script>...</script> survive WordPress's wp_kses_post on-save sanitization because kses does not decode HTML entities, and are only converted back into executable HTML tags at render time by the plugin's own shortcode filter. This requires snippet shortcodes to be enabled.	6.4	More Deta
CVE-2026-109975	The Cozy Blocks – Website Builder for WordPress Block Editor | Gutenberg Blocks, Patterns & Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'content (block attribute icon.view / icon.layout / icon.gap)' parameter in all versions up to, and including, 2.2.27 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. Although wp_kses_post is applied on save, it does not neutralize a quote-only attribute-breakout payload containing no '<' character, leaving the block comment and its decoded JSON attributes intact and exploitable at render time.	6.4	More Deta
CVE-2026-111727	The Appointment Booking Calendar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'vs_text_submitbtn' parameter in all versions up to, and including, 1.4.05 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This requires the attacker to be assigned as a calendar owner, a per-user grant that any administrator can extend to users as low as Subscriber level through the plugin's calendar list screen. Exploitation by attackers with subscriber-level access and above requires that an administrator has assigned the attacker's account as owner (`conwer`) of a calendar via the plugin's calendar list screen; the plugin's UI lists all registered users regardless of role, so a Subscriber can be assigned. On a default installation, where that is not configured, the vulnerability requires attackers with editor-level access and above.	6.4	More Deta
CVE-2026-103370	The Awesome Support – WordPress HelpDesk & Support Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'wpas_files' parameter in all versions up to, and including, 6.4.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with custom-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This vulnerability is only exploitable when the "Enable drag-n-drop uploader for ticket form" setting is enabled, as it is disabled by default.	6.4	More Deta
CVE-2026-116749	The VikRentCar Car Rental Management System plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'className' parameter in all versions up to, and including, 1.4.10 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. wp_kses_post() applied at save time does not neutralize the payload because the injection lands in an HTML-attribute context where only a raw double-quote is needed to break out, and block-comment JSON encoding of that quote is decoded back to a literal character by do_blocks() at render time.	6.4	More Deta
CVE-2026-119712	PipesHub before 0.10.0 contains a server-side request forgery vulnerability in ImageParser._fetch_single_url that allows attackers to make the indexing service fetch internal addresses by embedding image URLs in documents. Attackers can supply Markdown or HTML via uploads, synced mailboxes, or web connectors to reach loopback, private-network, or cloud metadata endpoints, with image responses embedded into indexed content.	6.4	More Deta
CVE-2026-118164	The If-So Dynamic Content – Elementor & All Page Builders Personalization plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'repeater[*][version_uid] (and many sibling fields: freeze-mode, cookie-input, ip-input, compare, utm-value, page-url-compare, group-name, custom, ...)' parameter in all versions up to, and including, 1.10.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Deta
CVE-2026-102918	The Redux Framework plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 4.5.15 via the multi_media field. This is due to the field's renderer printing the stored value into an href attribute, a hidden input value and an HTML element without escaping, while every neighbouring attribute in the same method is wrapped in esc_attr(). It is compounded by Redux_Extension_Users::user_meta_save() evaluating a field's 'permissions' requirement against a user id taken from the request body ('checkuser_id') rather than the current user, so a Subscriber can write a field declared for 'manage_options'. This makes it possible for authenticated attackers with Subscriber-level access and above to inject arbitrary web scripts into their own profile record that execute when an administrator views that user's profile in the dashboard. Requires a theme or plugin that registers a multi_media field through the Redux Users API.	6.4	More Deta
CVE-2026-67079	HCL BigFix AEX is affected by a Clickjacking vulnerability, which could allow an attacker to embed the application within a malicious web page or iframe and trick users into performing unintended actions, potentially leading to unauthorized transactions or changes to their accounts.	6.4	More Deta
CVE-2026-86391	Dell PowerProtect Data Domain Management Center, Feature Release versions 7.7.1.0 through 8.8, LTS2024 release versions 7.13.1.0 through 7.13.1.80, LTS2025 release versions 8.3.1.0 through 8.3.1.40, LTS2026 release versions 8.6.1.0 through 8.6.1.20, contain an Authentication Bypass by Spoofing vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Denial of service.	6.4	More Deta
CVE-2026-115707	Insertion of Sensitive Information into Externally-Accessible File or Directory (CWE-538) in Elastic Cloud Enterprise (ECE) can lead to privilege escalation via Retrieve Embedded Sensitive Data (CAPEC-37). After the ECE certificate rotation procedure runs, data that it retains contains platform credentials and certificate authority private keys, and lower-privileged platform components can read this data. An attacker who controls any host in the installation can use this data to get full control of the ECE control plane and of the deployments that it manages.	6.4	More Deta

CVE-2026-76780	The Beyondseo plugin for WordPress is vulnerable to unauthorized access in versions up to, and including, 1.3.6. This is due to the plugin permanently granting the 'rankingcoach_write_redirectManager' (and sibling rankingcoach_write_* module capabilities) to the Contributor role via BaseModule::defineCapabilities(), whose default role list includes 'contributor', combined with the module's REST endpoints (registered through BaseSubmoduleApi::registerRouteCreate/registerRouteEdit/registerRouteDelete) authorizing state-changing requests solely through checkPermissionsPost(), which only calls current_user_can('rankingcoach_write_<module>') and performs no admin capability, ownership, or additional nonce check inside the callback. This makes it possible for authenticated attackers, with Contributor-level access and above, to elevate their privileges to effectively that of an Administrator with respect to site-wide redirect management — creating, updating, or deleting 301/302 redirects that RedirectManagerHooks::handleRedirects() executes for every frontend visitor on template_redirect, allowing hijacking of arbitrary paths (including /checkout, /wp-login.	6.3	More Deta
CVE-2026-118129	A vulnerability was found in jeremyckahn Chitchatter up to f82538633813c854a81a8b2112a2f6ba17b39cbc. The affected element is the function isConfigMessageEvent of the file src/Bootstrap.tsx of the component PostMessage Handler. Performing a manipulation of the argument parentDomain results in improper authentication. Remote exploitation of the attack is possible. The exploit has been made public and could be used. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided. The patch is named e3babb5cd83bfe3b99f1d82358ac5c1ea8e8a688. It is recommended to apply a patch to fix this issue. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.	6.3	More Deta
CVE-2026-63121	Kubewarden policies is a collection of WebAssembly policies for securing and governing Kubernetes clusters. For versions provisionally classified as affected before 2.1.2, `trusted-repos-policy` compares an image's `registry` hostname against `reject lists` and `allow lists` case-sensitively even though `registry` DNS names are case-insensitive. An image with an uppercase or mixed-case `registry` hostname can miss a rejection rule for the equivalent lowercase host, so the admission policy accepts a resource whose container runtime pulls the same prohibited image. Only reject-list configurations have this bypass: allow-list configurations fail closed by over-denying differently cased hostnames. The security consequences depend on the configured rejection policy and deployment environment. This issue is fixed in version 2.1.2.	6.3	More Deta
CVE-2026-119665	WHartTest 2.2.0 through 2.8.1 contains a missing authorization vulnerability in ScheduledTaskViewSet and TaskExecutionViewSet that allows authenticated users to access other projects' tasks. Attackers can set project_pk to another project's sequential ID to modify, delete, or trigger scheduled tasks via run-now and read execution logs.	6.3	More Deta
CVE-2026-113576	Adobe Digital Editions is affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and gain unauthorized write access. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed.	6.3	More Deta
CVE-2026-54854	Contributor Privilege Escalation in Profile Builder <= 4.0.5 versions.	6.3	More Deta
CVE-2026-118577	A vulnerability was identified in maotoumao MusicFreeDesktop 0.0.6/0.0.7/0.0.8. Impacted is an unknown function of the component Request Forwarder. The manipulation leads to server-side request forgery. Remote exploitation of the attack is possible. The exploit is publicly available and might be used. The identifier of the patch is b0d3876247a0a64fa0e430e4b21870e41f503182. It is recommended to apply a patch to fix this issue.	6.3	More Deta
CVE-2026-55147	LORIS (Longitudinal Online Research and Imaging System) is a self-hosted web application that provides data- and project-management for neuroimaging research. In versions from 22.0.0 prior to 27.0.4 and from 28.0.0 prior to 28.0.2, the `API` for the `imaging_browser` module permits edits to imaging data without checking the frontend permissions that restrict editing in Imaging Browser. An authenticated `API` caller can therefore modify imaging data without the required edit authorization. Deployments that no longer use the `API` can disable it to remove access to this endpoint. This issue is fixed in versions 27.0.4 and 28.0.2.	6.3	More Deta
CVE-2026-104623	A security vulnerability exists in the authorization handling for the local (management) cluster shell feature of SUSE Rancher Manager 2.15.0 up to 2.15.3, 2.14.0 up to 2.14.7, 2.13.0 up to 2.13.11, 2.12.0 up to 2.12.15, 2.11.0 up to 2.11.19 and possible older versions. The authorization check that was introduced to protect this feature was not applied to every API route that can reach it, so an alternative request form reached the shell handler without the access check being evaluated. This could allow any authenticated users to run a pod on the management cluster.	6.3	More Deta
CVE-2026-114690	A flaw was found in GCC. An out-of-bounds memory access vulnerability exists in the libstdc++ parallel search implementation due to an undersized internal buffer. A local attacker can exploit this flaw by providing crafted search data to an application compiled with parallel mode, causing the process to crash and leading to a Denial of Service (DoS).	6.2	More Deta
CVE-2026-119134	Wasmtime before 36.0.18, 37.0.0 before 48.0.6, and 49.0.0 before 49.0.3 caps component-model resource handle tables only per component instance and does not charge handle allocations to any ResourceLimiter or StoreLimits. A malicious guest can repeatedly call resource.new and instantiate sub-components to exceed the per-instance cap many times over, causing unbounded host memory growth.	6.2	More Deta
CVE-2026-112356	GFI KerioConnect (Kerio Connect) before 10.0.9 Patch 2 contains a cross-site scripting vulnerability in the Webmail component that allows a remote attacker to spoof link targets or inject HTML into a message as rendered in a victim's authenticated Webmail session by sending a crafted email whose text is already inside a link. Attackers can exploit the link auto-formatter's re-processing of already-linked text, using quote characters to break out of the href attribute and inject attacker-controlled markup to execute script in the victim's session.	6.1	More Deta
CVE-2026-119601	AFFLIB through 3.7.22 contains a heap out-of-bounds write vulnerability in af_get_page() that allows attackers to corrupt heap memory by supplying crafted AFF images with mismatched page and sector sizes. Attackers can set a page size larger than and not a multiple of the sector size, causing the sector zero-fill loop to write past the buffer and crash forensic tools.	6.1	More Deta
CVE-2026-119761	Axigen Mail Server WebMail before 10.6.39 and 10.7.1 contains a stored cross-site scripting vulnerability that allows unauthenticated remote attackers to inject script via unescaped sender display names in the conversation view. Attackers can send an email with HTML and script in the From display name that executes when the recipient opens the folder, enabling mailbox content theft or redirection.	6.1	More Deta
CVE-2026-7004	WIT SynApps Runtime through 1.4.11 contains a pre-authentication reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject and execute arbitrary JavaScript by submitting a crafted LINK query parameter to the /System/Session-1 endpoint. Attackers can exploit this flaw to harvest credentials, manipulate the login flow, access browser-visible data, and perform same-origin requests to controller endpoints, including an origin-switch primitive against the internal controller in Cloud RIA scenarios.	6.1	More Deta
CVE-2026-92098	The Webheadcoder Multi-Step Forms for Contact Form 7 plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'l10n_print_after' parameter in all versions up to, and including, 4.7 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. Successful exploitation requires that the targeted site has at least one Contact Form 7 form configured with a [multistep] form-tag, as the canonicalization introduced in version 4.7 blocks the attack path on non-multistep forms.	6.1	More Deta
CVE-2026-7005	WIT SynApps Runtime through 1.4.11 contains a browser-mediated cross-origin request forgery vulnerability that allows attackers to supply an arbitrary target address during controller onboarding, causing the victim's browser to issue discovery requests to attacker-specified hosts at paths such as /easy/GUI/Skins/Default/SiteLogo and /easy/GUI/Skins/Default/Identity. Attackers can leverage the victim's browser reachability to probe loopback addresses, local hostnames, or internal-only network hosts and initiate the enrollment flow against REDY instances, crossing IT/OT	6.1	More Deta

	segmentation boundaries through a sanctioned application path.		
CVE-2026-117622	Jenkins 2.587 and earlier, LTS 2.580.1 and earlier allows agents to send exceptions implementing the Stapler HttpResponse interface to the controller, resulting in a cross-site scripting (XSS) vulnerability exploitable by attackers in control of agent processes.	6.1	More Deta
CVE-2026-117621	Jenkins 2.587 and earlier, LTS 2.580.1 and earlier computes on the agent the URL of the link shown in the workspace browser for each file and directory, resulting in a cross-site scripting (XSS) vulnerability exploitable by attackers in control of agent processes.	6.1	More Deta
CVE-2026-37468	Cross Site Scripting vulnerability in BeeHome MyBeeHome before 2025-11-01 allows a remote attacker to execute arbitrary code via the Profile editing functionality, chat messaging component.	6.1	More Deta
CVE-2026-118384	GNU mtools before 4.0.50 has an out-of-bounds write in parse_vses in vfat.c.	6.1	More Deta
CVE-2026-118656	Echo is a Go web framework. Prior to 4.16.0 and 5.4.0, sanitizeURI checks only the first two bytes of a redirect target before deciding whether it begins with an absolute-path separator pair. When AddTrailingSlash or RemoveTrailingSlash is configured with a redirect status, a slash, TAB, separator path form can evade the guard, be emitted in the Location header, and be normalized by a browser into an attacker-controlled host. This issue is fixed in 4.16.0 and 5.4.0.	6.1	More Deta
CVE-2026-91152	The Everest Forms – Contact Form, Payment Form, Quiz, Survey & Custom Form Builder with AI plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'evf_toast_type' parameter in all versions up to, and including, 3.6.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. Exploitation requires the sibling evf_toast parameter to decode successfully via atob(), but this is a trivially attacker-controlled prerequisite.	6.1	More Deta
CVE-2026-119721	Blender before 4.5.15 and 5.x before 5.2.3 contains an out-of-bounds read vulnerability in blo_bhead_id_* accessors in readfile.cc that read ID fields without block length checks. Attackers can supply a crafted .blend file with short ID blocks that, when browsed or appended from, causes heap over-reads leading to crashes or heap memory disclosure.	6.1	More Deta
CVE-2026-118652	Echo is a Go web framework. Prior to 4.16.0 and 5.4.0, Context.JSONP and Context.JSONPBlob concatenate an unvalidated callback value into a JavaScript response. A route that passes attacker-controlled input as the callback can return executable script syntax, allowing reflected cross-site scripting when a user loads the crafted response. The vulnerable jsonPBlob path performs no callback validation or escaping, and exploitation requires an application route that exposes attacker control over the callback argument. This issue is fixed in 4.16.0 and 5.4.0.	6.1	More Deta
CVE-2026-61573	AVideo is a video-sharing Platform. Prior to 8.1.0, the anonymous login interface reflects request values into HTML and JavaScript without output encoding. In `view/index.php`, `webSiteRootURL` is returned verbatim by `Streamer::getStreamerURL()` in `objects/Streamer.php` and reaches navigation and form attributes; it also enters a single-quoted JavaScript string in `view/index.header.php`. It is not filtered by `objects/security.php`, while the `user` and `pass` fields are filtered only for single quotes, leaving double quotes and angle brackets capable of breaking out of their HTML attributes. In addition, `view/index.header.php` reflects POST fields using `json_encode` without `JSON_HEX_TAG`, allowing a closing script tag to break out, and `locale/function.php` stores the POST `lang` value in the session for unescaped reflection in `view/index.php`. An unauthenticated remote attacker who persuades a victim to open a crafted login link can execute arbitrary JavaScript in the encoder's origin. This can read the operator session identifier exposed in inline script, capture login credentials and perform actions as the operator against the encoder and its upstream platform. This issue is fixed in version 8.1.0.	6.1	More Deta
CVE-2026-101935	The Echo Knowledge Base – Documentation, FAQs, Chat & Smart Search plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'new_kb_config' parameter (specifically the article-mobile-break-point-v2 key, among other config keys interpolated into the <style> element) in versions up to, and including, 17.214.0 This is due to insufficient input sanitization and output escaping in EPKB_Frontend_Editor::fe_preview_config() and EPKB_Articles_Setup: on every knowledge base article page view, when the request supplies epkb_fe_reload_mode=on, an attacker-controlled JSON blob is merged over the stored KB configuration and several values are concatenated directly into a stylesheet emitted inside a literal <style> element without escaping (minify_css() does not strip <, > or /). This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user (with Editor-level access or above, holding the manage_categories capability, or an Administrator) into performing an action such as clicking on a specially crafted link.	6.1	More Deta
CVE-2015-20130	Netsweeper before 4.0.11 and 4.1.0 before 4.1.5 contains a reflected cross-site scripting vulnerability in webadmin/reporter/view_server_log.php that allows remote attackers to execute arbitrary JavaScript by injecting malicious code through the log request parameter, which is reflected into the HTML response without output encoding. Attackers can craft a malicious URL and induce a user to request it, resulting in arbitrary JavaScript execution within the victim's browser session against the Netsweeper web administration interface. Exploitation evidence was first observed by the Shadowserver Foundation on 2023-10-19.	6.1	More Deta
CVE-2026-118766	Botan is a C++ cryptography library. Prior to 3.13.0, Botan's online OCSP client allowed a single HTTP redirect while posting an OCSP request to the URI in a certificate's Authority Information Access extension. A malicious OCSP responder or an on-path attacker could redirect the client to make one blind request to an otherwise unreachable internal HTTP service. The primary impact is blind SSRF that might affect internal services with non-idempotent GET handlers, and response timing can provide a coarse internal-service oracle. This issue is fixed in version 3.13.0.	6.1	More Deta
CVE-2026-104063	Scribus before 1.6.7 and 1.7.x before 1.7.4 contains an out-of-bounds read vulnerability in the Mac PICT image loader and import plugin when decoding planar pixel data. Attackers can supply a crafted PICT file with manipulated dimensions that, when placed or imported, causes heap over-reads leading to crashes or heap memory disclosure.	6.1	More Deta
CVE-2026-11854	The authentication endpoint generates an error message that includes reflected data directly from the request without sufficient sanitization or encoding. This allows an attacker to inject malicious scripts that can be executed in the context of a victim's browser. Successful exploitation enables an attacker to perform actions within the user's browser, such as redirecting the user to a malicious website, modifying the web page's user interface, or retrieving information. However, due to the httpOnly flag on session-related cookies, session hijacking or similar attacks are not possible.	6.1	More Deta
CVE-2026-117608	Assimp through 6.0.5 contains an integer overflow vulnerability in MD2Importer::ValidateHeader() that allows attackers to bypass frame table bounds checks using crafted header fields. Attackers can supply a malicious .md2 file whose numFrames and numVertices values wrap the 32-bit size check, causing heap out-of-bounds reads that crash applications or expose adjacent heap memory.	6.1	More Deta
CVE-2026-79656	A user with read access to Grafana's server logs, or to a log store they are shipped to, can recover the OAuth and OIDC access, refresh and ID tokens of users who sign in through the Generic OAuth, Google or GitLab providers. Grafana writes these tokens to its logs unredacted when an access or ID token is not a valid JWT, when the ID token is missing (at debug level) or is not a string (exposure of sensitive information in log files). The exposure is bounded by the scopes granted to the configured OAuth client.	6.0	More Deta

CVE-2026-118677	n8n before 2.41.4 and 2.42.x before 2.42.1 contains a missing confirmation vulnerability in the Local Gateway desktop app that allows its deep-link connect handler to silently re-pair the app with a different n8n instance. Attackers can lure users running the Local Gateway into opening a crafted n8n-computer-use:// link to connect their computer to an attacker-controlled instance, inheriting previously granted permissions and acting on the computer through the gateway.	5.9	More Deta
CVE-2026-119422	Juspay Hyperswitch before 1.128.0 contains an authentication bypass vulnerability that allows unauthenticated attackers to forge payment status updates because the Worldpayxml connector's verify_webhook_source always returns true without enforced mTLS. Attackers knowing the merchant_id and Worldpay orderCode can POST unsigned XML with lastEvent SETTLED to the worldpayxml webhook endpoint, marking unpaid payments as charged or triggering refund, dispute and payout events.	5.9	More Deta
CVE-2026-118593	A flaw was found in Red Hat Enterprise Linux 9 kernel builds. An incomplete backport of the CVE-2026-46099 fix in RHEL 9.6 through 9.10 left a local_bh imbalance in seg6_input_core(), where the drop path returns with bottom halves still disabled. This can lead to softirq starvation and denial of service on systems with SRv6 tunnels configured. Upstream and RHEL 10 are not affected.	5.9	More Deta
CVE-2026-119560	OPNsense core through 26.7.8 contains a configuration injection vulnerability that allows authenticated users to append ntpd.conf directives by embedding newlines in the fudge and refid fields. Attackers holding the page-services-ntp-gps or PPS privilege can submit CR/LF characters via services_ntpd_gps.php or services_ntpd_pps.php to inject directives loaded by ntpd running as root.	5.9	More Deta
CVE-2026-119051	flat through 6.0.1 contains an uncontrolled resource allocation vulnerability in unflatten() that allows attackers to create huge sparse arrays via unbounded numeric keys. Attackers can supply flattened keys such as a.4294967294, causing iteration with forEach, spread or JSON.stringify to block the Node.js event loop.	5.9	More Deta
CVE-2026-119421	Juspay Hyperswitch through 1.128.0 (and builds before 2026.10.19.0) contains a missing authorization vulnerability that allows unauthenticated attackers to confirm payouts with any client_secret via POST /payouts/{payout_id}/confirm. Attackers holding the merchant's publishable key and a payout_id can confirm payouts and overwrite amount, currency, connector, and routing fields to trigger unauthorized merchant payouts.	5.9	More Deta
CVE-2026-119557	n8n from 2.14.0 through 2.46.3 contains a path traversal vulnerability in the Databricks node that allows unauthenticated attackers to reach arbitrary Databricks API endpoints by injecting unencoded resource identifiers. Attackers can supply ../ sequences and query strings via webhook, chat, or form inputs mapped to spaceId, indexName, or filePath to read secrets using the stored credential.	5.9	More Deta
CVE-2026-119199	Nuxt is an open-source web development framework for Vue.js. From 3.0.0 until 4.6.3, the Nuxt development server can expose the Nitro 2 development bundle at <buildDir>/dev/index.mjs through Vite file serving when the server is reachable over HTTP. Nitro inlines private runtimeConfig values resolved at build time into that bundle, including secrets configured in nuxt.config, and Nuxt 4.6.0 and later also inline the generated development appSecret. The default localhost binding limits remote exposure, production builds and Nitro 3 are not affected, and runtime configuration supplied only through NUXT_* environment variables at server startup is not inlined. This issue is fixed in version 4.6.3.	5.9	More Deta
CVE-2026-119299	gopacket provides packet processing capabilities for Go. Prior to 1.7.2, the SCTP chunk chain in layers/sctp.go passes attacker-controlled declared lengths and counts to decodeSCTPInit, decodeSCTPShutdown, decodeSCTPError, decodeSCTPSack, and decodeSCTPParameter without checking that each chunk contains the fixed fields, parameter TLVs, gap acknowledgements, or duplicate TSNs those sub-decoders read. A crafted SCTP segment can therefore cause out-of-bounds or inverted slice panics; the panic can terminate applications that use gopacket.DecodeOptions.SkipDecodeRecovery, direct registered decoders, or DecodingLayerParser with IgnorePanic enabled, while the default recovery-enabled APIs convert it to a per-packet decode error. This is the SCTP sub-decoder residual named but not remediated by CVE-2026-65819, whose version 1.7.1 changes bounded the generic dispatcher but left these per-type reads and loops unchecked. The impact is availability only, with no data disclosure, modification, or allocation amplification. This issue is fixed in version 1.7.2.	5.9	More Deta
CVE-2026-119554	Moodle 5.3.0, 5.2.0 through 5.2.4, 5.1.0 through 5.1.8, 5.0.0 through 5.0.11, and through 4.5.15 contain an sql injection vulnerability in the External database enrolment plugin via course idnumber. Editing teachers can store a backslash-quote payload in idnumber that executes during scheduled sync on MySQL/MariaDB external databases, reading data and manipulating enrolment results.	5.9	More Deta
CVE-2026-119574	Traefik from 3.2.0 before 3.7.15 contains a data race in the experimental FastProxy that allows unauthenticated attackers to crash the process by abusing HTTP/1 protocol upgrades. Attackers can repeatedly open and abort upgraded connections such as WebSocket, corrupting the unsynchronized shared bufio.Reader and triggering an unrecovered panic that terminates Traefik.	5.9	More Deta
CVE-2026-119559	OpenLiteSpeed through 1.9.4 contains an authentication bypass vulnerability that allows unauthenticated remote attackers to evade virtual host client certificate requirements over HTTP/3. Because QuicStream inherits a verifyContext() implementation that always returns true, attackers can present a non-mTLS host's SNI with a protected Host header to access protected content.	5.9	More Deta
CVE-2026-118657	Echo is a Go web framework. Prior to 4.16.0 and 5.4.0, Context.Scheme unconditionally trusts forwarded scheme headers from any client. A client that reaches Echo directly over plaintext HTTP can claim an HTTPS scheme and bypass HTTPSRedirect because the request is treated as already secure. Separately, behind a TLS-terminating proxy that passes an attacker-controlled header, a claimed HTTP scheme can suppress the Strict-Transport-Security header even though the browser receives the response over HTTPS. The practical risk is reduced when a trusted proxy overwrites the headers and direct backend access is prevented, but the framework previously had no trusted-source configuration for this decision. This issue is fixed in 4.16.0 and 5.4.0.	5.9	More Deta
CVE-2026-118684	MONAI before 1.6.1 contains an insufficient integrity verification vulnerability in check_hash() that silently returns True when hash_val is None, with MD5 as the default hash type. Attackers performing man-in-the-middle or registry compromise can substitute bundles, datasets, or model archives downloaded without hashes, enabling malicious file delivery and potential code execution.	5.9	More Deta
CVE-2026-118370	libexpat through 2.9.0 contains a signed integer overflow vulnerability in storeAtts() in lib/xmlparse.c that allows attackers to trigger out-of-bounds writes via oversized attribute counts. Attackers can supply a multi-gigabyte document with a start tag carrying over 2^30 attributes to overflow attIndex and nPrefixes, crashing applications or corrupting heap memory.	5.9	More Deta
CVE-2026-119279	MariaDB Connector/J is used to connect applications developed in Java to MariaDB and MySQL databases. From 3.0.0 until 3.3.7, 3.4.5, and 3.5.10, the ReadableByteBuf.readLength() and ReadableByteBuf.readIntLengthEncodedNotNull() methods narrowed the protocol's unsigned 8-byte length-encoded integer to a Java int without checking that the value fit a non-negative integer. Values above Integer.MAX_VALUE could wrap to a negative or unrelated length that downstream allocation and read paths used. A malicious or compromised server, or a machine-in-the-middle attacker, could trigger NegativeArraySizeException, out-of-bounds failures, or oversized allocation behavior in client connection handling. This issue is fixed in versions 3.3.7, 3.4.5, and 3.5.10.	5.9	More Deta
CVE-2026-118778	Forge (also called node-forge) is a native implementation of Transport Layer Security in JavaScript. Prior to 1.4.1, the affected implementation used forge.tls.createConnection(), c.session.serverCertificate, RSA key exchange to process the relevant input or security decision. node-forge's TLS client checked the wrong property when deciding whether a server certificate was missing. A malicious TLS server or on-path peer could omit the Certificate message and reach code that dereferenced the absent certificate, causing an uncaught exception and terminating the connection or process. This issue is fixed in version 1.4.1.	5.9	More Deta
CVE-	MariaDB Connector/J is used to connect applications developed in Java to MariaDB and MySQL databases. From 3.0.0 until 3.3.7, 3.4.5, and 3.5.11, the connector assumed result bytes were UTF-8 but guarded only changes to character_set_client. It did not reject non-UTF-8 character_set_results changes and relied on the server's global session_track_system_variables configuration to report character-set changes. A malicious or		More

2026-119281	compromised server, or a machine-in-the-middle attacker, could suppress tracking or change the result charset so application strings differed from the returned bytes, potentially defeating application-side validation or escaping that depended on the decoded values. This issue is fixed in versions 3.3.7, 3.4.5, and 3.5.11.	5.9	Deta
CVE-2026-107250	Vulnerability in Drupal ECA Helper. This issue affects ECA Helper versions: *.*.	5.9	More Deta
CVE-2026-119285	Fiber is an Express inspired web framework written in Go. From 2.52.1 until 2.52.3, the CORS middleware's validateDomain wildcard matcher in middleware/cors/utils.go strips the scheme and checks only a host suffix without requiring a dot boundary. An application configured with a wildcard-subdomain AllowOrigins value and AllowCredentials enabled can reflect an unrelated attacker-controlled origin whose host merely ends with the configured base domain. A user who visits that origin can expose authenticated cross-origin responses to the attacker's page; empty-label origins and later comma-space parsing hardening are outside this advisory. This issue is fixed in version 2.52.3.	5.9	More Deta
CVE-2026-119278	MariaDB Connector/J is used to connect applications developed in Java to MariaDB and MySQL databases. From 3.0.0 until 3.3.7 and 3.4.5, during caching_sha2_password authentication, the authentication-more-data response was treated as a length-encoded byte array, memory was allocated from the server-declared length, and authResult[0] was accessed without ensuring a byte existed. A malicious or compromised server, or a machine-in-the-middle attacker, could declare a very large length or send an empty response before any password was transmitted. The malformed packet could cause excessive allocation or an unchecked ArrayIndexOutOfBoundsException escaping from DriverManager.getConnection(). This issue is fixed in versions 3.3.7 and 3.4.5.	5.9	More Deta
CVE-2026-117610	libexpat through 2.9.0 contains a NULL pointer dereference vulnerability in externalEntityInitProcessor2() in lib/xmlparse.c that mishandles the XML_TOK_NONE token from empty input. Attackers who control stream chunking can force an empty non-final first parse on an external entity subparser, causing a later parse to crash the application.	5.9	More Deta
CVE-2026-119277	MariaDB Connector/J is used to connect applications developed in Java to MariaDB and MySQL databases. From 3.0.0 until 3.3.7, 3.4.5, and 3.5.11, decoders for OK packet session-state blocks, column definition packets, text row data, or binary row data used server-declared lengths without confirming that the requested bytes remained in the receive buffer. The decoders could position reads, create sub-buffers, or decode strings beyond the packet boundary. A malicious or compromised server, or a machine-in-the-middle attacker, could trigger unchecked ArrayIndexOutOfBoundsException or IllegalArgumentException failures inside JDBC calls and terminate connection handling. This issue is fixed in versions 3.3.7, 3.4.5, and 3.5.11.	5.9	More Deta
CVE-2026-119276	MariaDB Connector/J is used to connect applications developed in Java to MariaDB and MySQL databases. From 3.0.0 until 3.3.7, 3.4.5, and 3.5.11, when CLIENT_SESSION_TRACK was negotiated, the OkPacket.parse() and OkPacket.parseWithInfo() paths allocated byte arrays using server-declared lengths for the OK packet info field and session-state variable names and values before confirming that the bytes remained in the packet. A malicious or compromised server, or a machine-in-the-middle attacker, could send a small OK packet declaring a much larger length and repeatedly force attacker-controlled heap allocations before the subsequent copy failed. This could create garbage-collection pressure or an OutOfMemoryError in the client application. This issue is fixed in versions 3.3.7, 3.4.5, and 3.5.11.	5.9	More Deta
CVE-2026-118374	LibreSSL ocspcheck through 4.4.0 contains a memory exhaustion vulnerability that allows malicious OCSP responders to exhaust memory by sending unbounded HTTP responses. Attackers controlling the responder or intercepting plain HTTP AIA OCSP traffic can stream endless headers or body data to http_head_read() and http_body_read(), denying certificate status checks.	5.9	More Deta
CVE-2026-110185	The Bit Flows: AI Agent Automation & Integrations for Forms, CRM, eCommerce, Google Sheets, and More plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.31.0 via the 'image (any body field referenced by the ImageHelper node's mix tag)' 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. Exploitation requires that an administrator has built a webhook-triggered flow that pipes a webhook body field into an ImageHelper imageToBase64 node, and that the webhook remains in its default configuration (no bearer secret enforced, no IP allowlist set) — a legitimate and documented use case.	5.9	More Deta
CVE-2026-107253	Vulnerability in Drupal Orphans Media. This issue affects Orphans Media versions: *.*.	5.9	More Deta
CVE-2026-118655	Echo is a Go web framework. Prior to 4.15.3 and 5.2.0, middleware.Static can decode an already decoded Request.URL.Path a second time. Double-encoded separators can consequently be reconstructed before filesystem resolution. This can reach a file under a guarded route when the static middleware is registered globally. This issue is fixed in 4.15.3 and 5.2.0.	5.9	More Deta
CVE-2026-118654	Echo is a Go web framework. Prior to 4.16.0 and 5.4.0, Echo's static file handlers can normalize dot segments after route matching and serve a file through a public static route even though the corresponding direct path is protected by route-level middleware. An unauthenticated attacker can read files that an application intended to protect with route-level middleware, when those files are also reachable through a static filesystem mount after path normalization. This vulnerability is the result of an incomplete fix for CVE-2026-55677. This issue is fixed in 4.16.0 and 5.4.0.	5.9	More Deta
CVE-2026-118029	Unverified ownership of the default query result location in the Athena module in AWS SDK for pandas (awswrangler) before 3.16.1 might allow remote actors to read Athena query results and tamper with result sets returned to the caller via a pre-created S3 bucket. To remediate this issue, users should upgrade to version 3.16.1 or later. Users should also verify that the default Athena result bucket in each account and region is owned by their own account, and set an explicit result location or enforce a workgroup result configuration.	5.9	More Deta
CVE-2026-119186	Forge (also called node-forge) is a native implementation of Transport Layer Security in JavaScript. Prior to 1.4.1, node-forge did not validate the AES-GCM tagLength option passed to start() during decryption through forge.cipher.createDecipher(). When an application derived tagLength from received data or used an unset or zero-like configuration value, a value that converted to zero together with an empty or missing authentication tag caused the calculated and supplied tags to compare as empty, so decipher.finish() accepted unauthenticated ciphertext. Applications that omit tagLength to use the 128-bit default or pass a fixed valid tag length are unaffected. This issue is fixed in version 1.4.1.	5.9	More Deta
CVE-2026-62303	Pistache is a high-performance REST toolkit written in C++. From 0.0.5 through 0.4.26, `SegmentTreeNode::sanitizeResource()` in `src/server/router.cc` uses `std::regex_replace()` with the `//+` expression to collapse consecutive slashes. With libstdc++, a path containing tens of thousands of consecutive slash characters can recurse deeply enough to exhaust the stack and crash the process. `Router::route()`, `Router::addRoute()` and `Router::removeRoute()` reach this normalization. Unauthenticated remote exploitation is conditional on a deployment allowing sufficiently long request paths, such as by increasing `Endpoint::Options::maxRequestSize()` above the default 4096-byte limit or forwarding long paths through a front end. Direct router API use is also affected when attacker-controlled route or resource strings reach the normalizer. Native builds reproduced a crash around 24,000 consecutive slashes, although the exact threshold depends on the stack and standard library; the demonstrated failure is stack exhaustion rather than uninitialized-memory use. A source fix replaces recursive regular-expression normalization with an iterative pass, but no containing repository release was verified as of time of publication.	5.9	More Deta
	Forge (also called node-forge) is a native implementation of Transport Layer Security in JavaScript. Prior to 1.4.1, node-forge enforced an X.509 CA		

CVE-2026-119189	certificate's basicConstraints.pathLenConstraint only when that certificate also carried a keyUsage extension. Exploitation requires a path-length-constrained CA without keyUsage that chains to a root trusted by the application, and an attacker who holds that CA's private key or obtains a subordinate CA certificate from it. The attacker could then construct a chain exceeding the declared path length that still passed pki.verifyCertificateChain(). Public web PKI CA certificates normally include keyUsage; private PKIs with CA certificates created without it are more likely to be affected. This issue is fixed in version 1.4.1.	5.9	More Deta
CVE-2026-114691	A flaw was found in the libstdc++ component of GCC. An attacker who can provide an excessively large element count to a boolean vector (std::vector<bool>) constructor can trigger an integer wrap during internal memory calculations. This issue leaves the container in an inconsistent state, leading to out-of-bounds memory access and resulting in an application crash or a Denial of Service (DoS) during subsequent operations.	5.9	More Deta
CVE-2014-125136	C97net qEngine CMS through 6.0.0, Kemana Directory through 1.5.6, and Cart Engine through 3.0.0 contain an information disclosure vulnerability that exposes database backups in the web-accessible /admin/backup directory. Unauthenticated attackers can list the directory or guess date-based names like 'Full Backup YYYYMMDD.sql' to download dumps containing user records and administrator password hashes.	5.9	More Deta
CVE-2026-119198	Nuxt is an open-source web development framework for Vue.js. From 4.6.0 until 4.6.3, a client with TCP access to an exposed Nuxt development server can send a nuxt:dev:client-error event over the HMR socket with an absolute file path at the end of its message. The development server reads that file while building the client error report and returns its contents through the error overlay, development error channel, and terminal report, bypassing Vite's server.fs allow list. The default localhost binding limits remote exposure, cross-origin browser requests are rejected, production builds and Nuxt 3 are not affected, and no browser interaction is required. This issue is fixed in version 4.6.3.	5.9	More Deta
CVE-2026-119210	MariaDB Connector/J is used to connect applications developed in Java to MariaDB and MySQL databases. From 3.0.0 until 3.3.7, 3.4.5, and 3.5.11, the ClientMessage.validateLocalFileName() check used a regular expression that could match LOAD DATA LOCAL INFILE text inside quoted identifiers, string literals, or comments instead of requiring a real statement. A malicious or compromised server, or a machine-in-the-middle attacker, could return crafted database or table identifiers that the connector reused in metadata or updatable-result queries, then answer with a LOCAL INFILE request for a client file. With allowLocalInfile enabled, this caused the connector to stream any readable client-host file named by the crafted text, including through DatabaseMetaData.getImportedKeys(), DatabaseMetaData.getExportedKeys(), or ResultSet.updateRow() paths. This issue is fixed in versions 3.3.7, 3.4.5, and 3.5.11.	5.9	More Deta
CVE-2026-115225	The Customer Engagement System WordPress plugin before 2.0.2 does not restrict access to its MailChimp interest-group lookup or validate the API key supplied to it, allowing unauthenticated users to make the server open connections to arbitrary internal hosts and ports and infer from response timing which ones are reachable.	5.8	More Deta
CVE-2026-110133	A flaw was found in Ghostscript. When processing a specially crafted TrueType font or document embedding one, an accounting error during font rendering can bypass buffer size checks, triggering a heap-based buffer overflow. A remote attacker could exploit this by enticing a victim or automated service to open the malicious content, potentially resulting in a Denial of Service (DoS) crash or arbitrary code execution.	5.8	More Deta
CVE-2026-119709	Grimoire before 1.0.0 contains an unauthenticated server-side request forgery vulnerability in the /api/fetch-metadata POST handler that passes user-supplied URLs to getMetadata() without authentication checks. Attackers can submit URLs targeting loopback, internal-network, or cloud metadata endpoints and read the parsed title, description, and page content returned.	5.8	More Deta
CVE-2026-103405	An Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') vulnerability in the web server in Juniper Networks Session Smart Router and Session Smart Conductor allows an attacker to inject arbitrary HTTP headers via unsanitized request body parameters.	5.8	More Deta
CVE-2026-105618	PostgreSQL Anonymizer's documentation recommends applying rules on partitions and inheritance tables. Direct access to the paritions / inheritance tables is masked but not thru the parent table. The problem is resolved in PostgreSQL Anonymizer 3.3.0 and later versions.	5.7	More Deta
CVE-2026-105616	PostgreSQL restricts acces to the salt and shift via the `SHOW` command for users not member of `pg_read_all_settings`. But they are visible in `pg_db_role_setting` or `pg_roles` if they were set on the database, user or both. PostgreSQL Anonymizer's documentation recommends to use ALTER DATABASE / ALTER ROLE for the salt. The problem is resolved in PostgreSQL Anonymizer 3.3.0 and later versions.	5.7	More Deta
CVE-2026-42949	A authorization bypass vulnerability exists in the /api/runscript functionality of FUXA (version(s): 1.3.2-2809). A specially crafted HTTP request can lead to execute priviledged operation. An attacker can make an unauthenticated HTTP request to trigger this vulnerability.	5.6	More Deta
CVE-2026-119146	ProFTPD before 1.3.9e and 1.3.10rc5 contains a buffer overflow vulnerability in the mod_rewrite int:utf8trans RewriteMap that allows remote attackers to overwrite static buffers. Attackers can send FTP command arguments longer than 1024 bytes, without authentication if pre-login commands are rewritten, to corrupt session memory and crash the session.	5.6	More Deta
CVE-2026-118984	OmniRoute 3.8.0 before 3.8.52 contains an unverified password change vulnerability that allows holders of manage- or admin-scoped API keys or oma_ access tokens to change the management password without the current password. Attackers can send POST requests to /api/settings/require-login to lock out the operator, take over dashboard login, or disable the login requirement entirely.	5.5	More Deta
CVE-2026-119207	pypdf is a free and open-source pure-python PDF library. Prior to 6.21.3, pypdf can consume excessive memory when strict mode loads a crafted invalid PDF dictionary. Nested parsing failures add repeated exception text to newly raised errors, allowing a small malformed dictionary to amplify into very large error messages. This issue is fixed in version 6.21.3.	5.5	More Deta
CVE-2026-119205	pypdf is a free and open-source pure-python PDF library. Prior to 6.21.4, pypdf can enter an infinite loop when cloning or duplicating a crafted cyclic DictionaryObject. Clone traversal checked generated destination references rather than the original source references, allowing some source cycles to evade the visited-object check. This issue is fixed in version 6.21.4.	5.5	More Deta
CVE-2026-93516	A use-after-free caused by lack of lifecycle management when adding / removing XInput master devices in X.org X Server before 21.1.25 and XWayland before 24.1.14 could be used by authenticated X Clients to crash the X server or potentially execute code in X server context.	5.5	More Deta
CVE-2026-119204	pypdf is a free and open-source pure-python PDF library. Prior to 6.21.4, pypdf can consume excessive memory while parsing a crafted PDF page tree containing many shared resources. Page-tree flattening copies page dictionary and inherited resource entries without a document-wide entry budget, allowing the crafted resource structure to cause disproportionate allocations. This issue is fixed in version 6.21.4.	5.5	More Deta
CVE-2026-119591	SQLite before 3.54.0 contains a stack exhaustion vulnerability in countOfViewOptimization() that allows attackers to crash the host process via count(*) over a large multi-row VALUES clause. Attackers supplying SQL or a database file with a crafted view can trigger deeply nested TK_PLUS expressions whose recursive freeing in sqlite3ExprDeleteNN() exhausts the C stack, causing denial of service.	5.5	More Deta
CVE-2026-119291	Zuke is a code-first, strongly typed build automation system for Deno. Prior to 1.4.0, @zuke/cli uses lstat to inspect scaffold names but then performs link-following reads, writes, and permission changes in zuke setup and zuke import. An attacker who supplies an untrusted cloned repository, template, or archive with a symbolic link at a scaffolded name can cause setup to overwrite a target outside the selected directory with the invoking user's permissions. The .gitignore path requires no flag, while --force permits a linked launcher target to be written and made	5.5	More Deta

	executable; import can also read link-target content and incorporate it into the generated build file. This issue is fixed in version 1.4.0.		
CVE-2026-118538	A vulnerability was determined in a2ui-project a2ui up to 0.12.0. This issue affects the function Root.renderComponentTree of the file src/0.8/ui/root.js of the component Renderer. Executing a manipulation can lead to dynamically-determined object attributes. The attack may be launched remotely. The pull request to fix this issue awaits acceptance.	5.5	More Deta
CVE-2026-119371	SQLite before 3.54.0 contains a stack exhaustion vulnerability that allows attackers to bypass the SQLITE_LIMIT_EXPR_DEPTH nesting limit because common table expressions are not counted against it. Attackers can supply a WITH clause chaining tens of thousands of CTEs, via plain SQL or a view in an untrusted database file, causing unbounded selectExpander() recursion that crashes the process.	5.5	More Deta
CVE-2026-118989	WebToffee Product Import Export for WooCommerce 2.5.1 before 2.6.8 contains a server-side request forgery vulnerability in download_remote_file that allows shop_manager users to reach internal services via redirects. Attackers can submit a .csv URL that returns an HTTP 302 redirect to an internal address, causing the server to fetch internal responses and return them as import data.	5.5	More Deta
CVE-2026-119372	SQLite before 3.54.0 built with FTS3/FTS4 and SQLITE_ENABLE_FTS3_PARENTHESIS contains a use-after-free vulnerability in fts3BestSnippet() caused by dangling cached position-list pointers. Attackers can run a full-text MATCH query combining OR and NEAR operators with snippet() to read freed heap memory and crash the process.	5.5	More Deta
CVE-2026-62250	LibreDWG is a free C library to read and write DWG files. Prior to 0.14.8413, a crafted pre-R13 DWG can make `decode_preR13_entities()` in `src/decode.c` enter a nonterminating loop that allocates a new object each iteration. `decode_preR13` in `src/decode_r11.c` computes `size` from the raw file-controlled `entities_start` and `entities_end` header bounds; the callee clamps `end` to `dat->size` but never recalculates `size`. At `end` of input, `bit_read_RC` and `bit_read_RS` stop advancing `dat->byte`, the overflow guard fails because `end` equals `dat->size`, and the no-advance check compares against `oldpos` saved before the loop instead of the previous iteration. This leaves repeated allocation of `dwg->object` entries until allocation fails or the process is OOM-killed, not merely a constant-memory CPU hang. The defect remains after the clamping and no-progress changes associated with the earlier issue 1131. Applications and tools calling `dwg_read_file()` on untrusted files, including `dwg2dxf`, `dwgread` and `dwg2svg`, can suffer denial of service when a user or automated pipeline opens a malformed file; no attacker credentials are required. This issue is fixed in repository nightly version 0.14.8413.	5.5	More Deta
CVE-2026-62254	LibreDWG is a free C library to read and write DWG files. Prior to 0.14, a specially crafted R13-R2000 DWG can trigger algorithmic resource exhaustion in `decode_R13_R2000` in `src/decode.c`. The class-decoding loop performs `realloc` on every iteration without a sanity check on `num_classes`. Manipulating that field forces an extremely slow allocation loop and denial of service when the file is parsed. Running the parser in a sandbox with memory limits is a workaround rather than a remediation. This issue is fixed in version 0.14.	5.5	More Deta
CVE-2026-118756	gopass before 1.17.0 contains a path traversal vulnerability in the filesystem storage backend that allows attackers to delete directories outside the password store via ../ entry names in Prune and IsDir. Collaborators with write access to a shared git-synced store can introduce crafted entries, causing a victim's recursive gopass rm -r to delete arbitrary directory trees.	5.5	More Deta
CVE-2026-119378	SQLite before 3.54.0 contains a use-after-free vulnerability in the R-Tree extension that allows attackers to make applications use freed heap memory by manipulating the %_node shadow table. Attackers can supply a database declaring %_node WITHOUT ROWID or with a RAISE(IGNORE) trigger so nodeWrite() hashes nodes as 0, crashing the process after node splits.	5.5	More Deta
CVE-2026-119375	SQLite before 3.54.0 contains an information disclosure vulnerability that allows attackers to read uninitialized page-cache memory by supplying a WAL file with an undersized page size. Attackers can craft a database and WAL file whose oversized record payload makes queries like substr() return stale bytes, disclosing other table rows and internal pointers.	5.5	More Deta
CVE-2026-119206	pypdf is a free and open-source pure-python PDF library. Prior to 6.21.3, pypdf can take excessive time to retrieve page labels from a crafted PDF containing a flat page-label number tree with many ranges. The page_labels property resolves each page independently and repeatedly scans the same /Nums array from the beginning, causing work to grow with both the page count and the number of label ranges. This issue is fixed in version 6.21.3.	5.5	More Deta
CVE-2026-119203	pypdf is a free and open-source pure-python PDF library. Prior to 6.21.4, pypdf can enter an infinite loop while opening a crafted incomplete PDF whose standard cross-reference table reaches the end of the file without a trailer. The trailer search can repeatedly rewind to the same stream position instead of terminating when parsing makes no progress, blocking the processing thread. This issue is fixed in version 6.21.4.	5.5	More Deta
CVE-2026-119208	pypdf is a free and open-source pure-python PDF library. Prior to 6.21.3, pypdf can consume excessive time and memory when an application accesses the page count of a crafted encrypted PDF whose page tree declares a forged /Count value. Even after successful decryption, page-count retrieval trusts the unvalidated declared count instead of walking the page tree, allowing the attacker-controlled value to drive excessive work and memory use. This issue is fixed in version 6.21.3.	5.5	More Deta
CVE-2026-111499	Dell OpenManage Enterprise, versions prior to 4.8.0, contains an Incorrect Permission Assignment for Critical Resource vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Protection mechanism bypass.	5.5	More Deta
CVE-2026-119546	Forgejo through 15.0.11, 16.0.0 through 16.0.7, and 17.0.0 through 17.0.1 contains a path traversal vulnerability in restore-repo that allows attackers to read files outside the dump directory via crafted asset paths. Attackers can supply a dump whose release.yml DownloadURL or PatchURL contains ../ sequences, importing files like app.ini as release attachments when an administrator restores it.	5.5	More Deta
CVE-2026-119720	Blender before 4.5.15 and 5.x before 5.2.3 contains a heap out-of-bounds read vulnerability in read_file_dna() that reads a GLOB block field without validating its declared length. Attackers can supply a crafted .blend file with a truncated GLOB block that, when opened, triggers the out-of-bounds read and crashes Blender.	5.5	More Deta
CVE-2026-119209	pypdf is a free and open-source pure-python PDF library. Prior to 6.21.3, pypdf can consume excessive memory while opening a crafted PDF containing cross-reference streams that declare very large entry counts. Highly compressible streams and /Prev chains can multiply the number of parsed entries across a document, while negative /Index counts can bypass the existing per-stream clamp. This issue is fixed in version 6.21.3.	5.5	More Deta
CVE-2026-103400	An Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') vulnerability in the ember service in Juniper Networks Session Smart Router and Session Smart Conductor allows an attacker with local access to unmount arbitrary filesystems or cause a denial of service via the creation of specially named directories and a service restart.	5.5	More Deta
CVE-2026-119340	Tesseract is an open source OCR engine. Prior to 5.5.4, GENERIC_2D_ARRAY::DeSerializeSize in src/ccstruct/matrix.h reads matrix dimensions as signed int32_t values and compares them only with UINT16_MAX, allowing negative values to reach ResizeNoInit. Negative dimensions or a 65535 by 65535 product can create inconsistent allocation state and later out-of-bounds accesses while loading a crafted traineddata file, causing denial of service. This issue is fixed in version 5.5.4.	5.5	More Deta
CVE-2026-119339	Tesseract is an open source OCR engine. Prior to 5.5.4, WeightMatrix::DeSerialize trusts a mode byte from a traineddata LSTM network and calls WeightMatrix::DeSerializeOld when kDoubleFlag is clear. In default FAST_FLOAT builds, DeSerializeOld invokes ASSERT_HOST instead of returning an error, so loading a crafted model through TessBaseAPI::Init terminates the process and causes denial of service. This issue is fixed in version 5.5.4.	5.5	More Deta

CVE-2026-119376	SQLite before 3.54.0 contains a stack exhaustion vulnerability that allows attackers to bypass the SQLITE_LIMIT_EXPR_DEPTH limit by chaining COLLATE postfix operators. Attackers can supply roughly 175,000 chained COLLATE operators in SQL or an untrusted database view to trigger unbounded recursion in sqlite3WalkExprNN() and crash the process.	5.5	More Deta
CVE-2026-118640	n8n before 1.123.85, 2.43.5, and 2.44.1 contains an authorization bypass vulnerability in Chat Hub that allows chat-only users to register restricted tool types. Users with the global:chatUser role can add and run tools through chat to execute sandboxed code, access permitted files, and use instance workflows, Data Tables, and agents.	5.4	More Deta
CVE-2025-13050	Broken Function Level Authorization allows execution of poller post-restart commands by authenticated user	5.4	More Deta
CVE-2026-119054	Multiple Pages Generator by Themeisle before 4.2.5 contains a stored cross-site scripting vulnerability that allows Contributor-level users to inject script via the [mpg] and [mpg_match] shortcode base-url attribute. Attackers can store entity-encoded payloads that pass kses but are decoded by html_entity_decode() and rendered unescaped through {{mpg_url}}, executing script in administrators' browsers.	5.4	More Deta
CVE-2026-119466	Cross-Site Request Forgery (CSRF) vulnerability in WPExperts APIExperts Square for WooCommerce woosquare allows Cross Site Request Forgery.This issue affects APIExperts Square for WooCommerce: from n/a through 4.7.5.	5.4	More Deta
CVE-2026-118959	A flaw was found in the required action provider mechanism of Keycloak. The issue occurs when an authorization request includes the kc_action query parameter set to a mandatory action already assigned to the user, such as profile verification or terms and conditions. Due to incorrect handling of application-initiated actions, Keycloak may skip these mandatory challenges and issue an authorization code. This can allow a user to bypass administrative requirements and gain access to the application without completing necessary profile updates or agreeing to terms.	5.4	More Deta
CVE-2026-114572	Authentication Bypass Using an Alternate Path or Channel vulnerability in Drupal Domain Login Restrict allows Authentication Bypass. This issue affects Domain Login Restrict versions: from 0.0.0 to 1.5.0.	5.4	More Deta
CVE-2026-62141	Missing Authorization vulnerability in WP ManageNinja LLC Fluent CRM fluent-crm allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Fluent CRM: from n/a through 3.2.6.	5.4	More Deta
CVE-2026-80069	MasterStudy LMS plugin for WordPress before 3.7.50 contains a missing authorization vulnerability that allows any authenticated user, including Subscribers, to trigger the stm_lms_send_test_email_ajax AJAX action without capability or nonce validation. Attackers can invoke this handler directly or via cross-site request forgery to cause an uncaught PHP fatal error that, when display_errors is enabled, discloses the absolute filesystem path of the plugin.	5.4	More Deta
CVE-2026-80067	MasterStudy LMS plugin for WordPress before 3.7.50 contains a path traversal vulnerability that allows authenticated Subscriber-level users to import arbitrary WXR XML files by supplying directory traversal sequences in the stm_lms_step parameter passed to the stm_lms_import_sample_data AJAX action, which lacks capability checks and nonce verification. Attackers can traverse the file system to reference a reachable WXR file and have the handler publish its contained posts under their identity, enabling publication of attacker-chosen post type, title, content, and metadata.	5.4	More Deta
CVE-2026-107252	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal MathJax: LaTeX for Drupal allows Cross-Site Scripting (XSS). This issue affects MathJax: LaTeX for Drupal versions: from 0.0.0 to 4.1.2.	5.4	More Deta
CVE-2026-109984	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, 7.5.55.7212 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 a site administrator to approve the comment containing the malicious shortcode; execution is then triggered for any visitor who interacts with the video player on that page.	5.4	More Deta
CVE-2026-118072	The Fraud Prevention For WooCommerce and EDD WordPress plugin before 2.3.6 does not check that a user is allowed to manage orders before letting them add an order's customer details to the store's fraud blacklist, which could allow users with the Subscriber role and above to prevent arbitrary legitimate customers from placing orders.	5.4	More Deta
CVE-2026-111500	Dell OpenManage Enterprise, versions prior to 4.8.0, contains a Missing Authentication for Critical Function vulnerability. An unauthenticated attacker with adjacent network access could potentially exploit this vulnerability, leading to Server-side request forgery.	5.4	More Deta
CVE-2026-117613	Jenkins 2.587 and earlier, LTS 2.580.1 and earlier does not restrict item types in collections after deserialization, allowing attackers with access to POST config.xml API endpoints to submit crafted `config.xml` files that can lead to, e.g., stored cross-site scripting (XSS) vulnerabilities.	5.4	More Deta
CVE-2026-117606	NexoPOS through 6.3.0 contains a missing authorization vulnerability that allows authenticated cashiers to manipulate other cashiers' register sessions because CashRegistersService never compares used_by with the user. Attackers holding the default nexopos.use.registers permission can submit closing, cash-in, or cash-out actions to POST /api/cash-registers/{action}/{register} to force-close sessions or alter balances.	5.4	More Deta
CVE-2026-118435	Out-of-bounds write vulnerability in Samsung Open Source escargot allows Buffer Manipulation.	5.4	More Deta
CVE-2026-42691	Authorization Bypass Through User-Controlled Key vulnerability in EventPrime EventPrime eventprime-event-calendar-management allows Privilege Abuse.This issue affects EventPrime: from n/a through 4.3.6.0.	5.4	More Deta
CVE-2026-116761	The CMB2 plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'cmb43ex1_grp[0][txt] (wysiwyg field inside group — field id controlled by integrator config)' parameter in all versions up to, and including, 2.13.4 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This is only exploitable when a site integrator renders the plugin's documented front-end form helper with a wysiwyg field inside a repeatable group on a publicly accessible page.	5.4	More Deta
CVE-2026-116407	Missing Authorization vulnerability in Webba Plugins Webba Booking webba-booking-lite allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Webba Booking: from n/a through 6.5.4.	5.4	More Deta

CVE-2026-100175	The Postie plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Email Body URL Autolink in all versions up to, and including, 1.9.87 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 ?postie=get-mail endpoint is reachable by unauthenticated users with no capability check, and the email processing path removes WordPress's kses output filters before saving raw markup, allowing the unescaped href attribute value to be stored as post content.	5.4	More Deta
CVE-2026-50542	Xibo is an open source digital signage platform with a web content management system and Windows display player software. Prior to 4.4.3, missing access-control checks on `GET /layout/status/{id}` allow an authenticated user with any privileges to view the `status and metadata` of any layout, including layouts for which the user does not have view rights. This issue is fixed in version 4.4.3.	5.4	More Deta
CVE-2026-16020	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Fazile BACAK DefterAsist Financial Advisor Platform allows Stored XSS. This issue affects DefterAsist Financial Advisor Platform: through 2026-10-27.	5.4	More Deta
CVE-2026-119367	Missing Authorization vulnerability in Liquid Web / StellarWP The Events Calendar the-events-calendar allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects The Events Calendar: from n/a through 6.18.2.	5.4	More Deta
CVE-2026-110001	The FV Flowplayer Video Player plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'comment (shortcode attribute 'align')' parameter in all versions up to, and including, 7.5.55.7212 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 plugin's 'Parse Vimeo and YouTube links' (parse_comments) setting to be enabled by an administrator, which causes the plugin to register do_shortcode on the comment_text filter, allowing attacker-supplied shortcode attributes stored in comments to be rendered unescaped to all subsequent visitors.	5.4	More Deta
CVE-2026-117627	A flaw was found in the JWT Authorization Grant implementation of the keycloak-services component. When an OIDC or Google identity provider is configured with specific login restrictions, such as claim filtering, these checks are correctly applied during standard browser logins but are skipped during the JWT-based grant flow. This allows an authenticated client to obtain access tokens for a user even if their identity provider claims should have blocked the login.	5.4	More Deta
CVE-2026-88090	Access of resource using incompatible type ('type confusion') in Microsoft Edge (Chromium-based) allows an unauthorized attacker to elevate privileges over a network.	5.4	More Deta
CVE-2026-104331	IBM Langflow OSS 1.0.0 through 1.12.3 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks.	5.4	More Deta
CVE-2026-111501	Dell OpenManage Enterprise, versions prior to 4.8.0, contains an Improper Restriction of Excessive Authentication Attempts vulnerability. An unauthenticated attacker with adjacent network access could potentially exploit this vulnerability, leading to Launch of phishing attacks.	5.4	More Deta
CVE-2026-119659	Blossom through 1.17.1 contains an authorization bypass vulnerability that allows authenticated users to access other users' folders because FolderService queries filter only on folder id. Attackers can supply another user's folder id to /folder/info, /folder/upd, /folder/open or /folder/del to read storage paths, rename, toggle visibility, or delete folders.	5.4	More Deta
CVE-2026-119563	phpMyAdmin through 5.2.3 contains a stored cross-site scripting vulnerability that allows database users with CREATE privilege to inject script via unescaped table names in DesignerHistory.display(). Attackers can create a table whose name contains HTML markup that executes in another user's session when they add a condition on it in Designer query mode.	5.4	More Deta
CVE-2026-119425	OPNsense core 26.1.6 through 26.7.7 contains an authentication bypass vulnerability in the captive portal roaming feature that lets unauthenticated attackers hijack authorized client sessions by spoofing unauthenticated MAC-to-IP observations. Attackers on the same Layer-2 segment can send forged gratuitous ARP replies binding their IP to a victim's MAC, gaining portal access with traffic attributed to the victim.	5.4	More Deta
CVE-2026-117859	A flaw was found in the Pushed Authorization Request PAR implementation of the keycloak-services component. The issue occurs when an authentication flow is restarted, which incorrectly clears the internal markers used to track PAR consumption while leaving the request active. This allows an attacker to reuse the same authorization request to obtain multiple access tokens, bypassing security requirements for single-use requests.	5.4	More Deta
CVE-2026-107265	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Leaflet allows Stored XSS. This issue affects Leaflet versions: from 0.0.0 to 10.4.13.	5.4	More Deta
CVE-2026-107629	The Greenshift – animation and page builder blocks plugin for WordPress is vulnerable to Stored DOM-Based Cross-Site Scripting via the 'comment' parameter in all versions up to, and including, 13.2.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Exploitation requires the affected post page to include an Advanced HTML Element block with Split Text animation enabled wrapping a Latest Comments block that displays comment excerpts, as this configuration causes splittext.js to be enqueued and to process the comment content container.	5.4	More Deta
CVE-2026-116855	Missing Authorization vulnerability in wphocus My auctions allegro my-auctions-allegro-free-edition allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects My auctions allegro: from n/a through 4.0.3.	5.4	More Deta
CVE-2026-119650	HuLa-Server through 3.0.7 contains an insecure direct object reference vulnerability in PrivacyController that allows authenticated users to access other users' privacy settings by supplying their uid. Attackers can send GET or POST requests to /privacy with a target uid parameter to read and overwrite that user's UserPrivacy settings without ownership checks.	5.4	More Deta
CVE-2026-119651	HuLa-Server through 3.0.7 contains an insecure direct object reference vulnerability in FeedController.delFeed that allows authenticated users to delete other users' moments by supplying arbitrary feedId values. Attackers can send POST requests to /feed/del with another user's feedId to delete their moments along with associated media, comments, and likes.	5.4	More Deta
CVE-2026-107264	Improper Neutralization of Special Elements Used in a Template Engine vulnerability in Drupal Inline Formatter Field allows Code Injection. This issue affects Inline Formatter Field versions: from 0.0.0 to 4.2.0.	5.4	More Deta
CVE-2026-42690	Subscriber Broken Access Control in LearnPress <= 4.4.10 versions.	5.4	More Deta

CVE-2026-107263	Incorrect Authorization vulnerability in Drupal Gutenberg allows Forceful Browsing. This issue affects Gutenberg versions: from 0.0.0 to 2.15.0, from 3.0.0 to 3.0.7.	5.4	More Deta
CVE-2026-115299	The Contact Form by Supsystic WordPress plugin before 1.11.1 does not verify a CSRF nonce before saving its mail settings, allowing an attacker to overwrite the site's outbound mail configuration, including the SMTP server, its credentials and the notification recipient, by tricking a logged-in administrator into visiting a crafted page, which can route the Contact Form by Supsystic WordPress plugin before 1.11.1's contact-form notifications through infrastructure the attacker controls.	5.4	More Deta
CVE-2026-107627	The Greenshift – animation and page builder blocks plugin for WordPress is vulnerable to Stored DOM-Based Cross-Site Scripting via the 'comment' parameter in all versions up to, and including, 13.2.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Exploitation requires an administrator to have published a page containing a Text Animated block with Content set to Blocks, a Latest Comments block with excerpts enabled nested inside it, and at least one Animated Texts value configured — conditions that cause the gs-textanimate script to be enqueued and process the comment excerpts.	5.4	More Deta
CVE-2026-103485	The Extensions for Leaflet Map plugin for WordPress is vulnerable to Stored DOM-Based Cross-Site Scripting via the 'feature.properties[<template-token>]' parameter in all versions up to, and including, 5.4 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Exploitation requires that a site administrator has previously configured a public map using the [leaflet-map]+[leaflet-geojson]+[choropleth] shortcode combination whose GeoJSON src URL is one the attacker controls — for example, through compromise of an external data host, a subdomain takeover, or a site intentionally pointing at an attacker-hosted feed.	5.4	More Deta
CVE-2026-111318	The HT Mega Addons for Elementor – Elementor Widgets & Template Builder plugin for WordPress is vulnerable to Stored DOM-Based Cross-Site Scripting via the 'href attribute of <a> inside .htmega-tab-nav' parameter in all versions up to, and including, 3.2.7 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 a co-installed plugin such as wpDiscuz with its rich editor enabled whose markup allowlist permits span[class] and a[href] storage, an HT Mega Tabs widget present on the same page as the comment section, and a victim user click on the injected anchor link.	5.4	More Deta
CVE-2026-119644	Blossom through 1.17.1 contains an authorization bypass vulnerability that allows authenticated non-readonly users to modify other users' pictures by supplying arbitrary picture ids. Attackers can call the picture delete, /picture/del/batch, or /picture/star endpoints to permanently delete victims' images and stored files or change their star status.	5.4	More Deta
CVE-2026-107259	Improper Neutralization of Special Elements Used in a Template Engine vulnerability in Drupal Linked Field allows Code Injection. This issue affects Linked Field versions: from 0.0.0 to 1.8.0.	5.4	More Deta
CVE-2026-107258	Incorrect Authorization vulnerability in Drupal Inline Entity Form Dialog allows Forceful Browsing. This issue affects Inline Entity Form Dialog versions: from 0.0.0 to 1.0.6.	5.4	More Deta
CVE-2026-75520	Domoticz is a free, open source home automation system for Linux, Windows, macOS, and Raspberry Pi. Prior to 2026.3, the `udevices` JSON command handler, `Cmd_UpdateDevices` in `main/WebServerCmds.cpp`, performed no `session.rights` check before invoking a Lua parser script, while its sibling command handlers gate access by role. A low-privilege authenticated user could trigger execution of an existing operator-installed Lua parser script with attacker-controlled input through the `GET /json.htm` endpoint with `type=command` and `param=udevices`. The `script` parameter also lacked a `..` path-traversal guard: `CLuaHandler::executeLuaScript` in `main/LuaHandler.cpp` constructed the filename from the parser directory and the supplied script name before passing it to `luaL_loadfile`. Execution is limited to already-installed valid Lua files; this is not arbitrary code execution, and the advisory states that file-write and upload paths require administrator privileges. This issue is addressed in version 2026.3.	5.4	More Deta
CVE-2026-116763	The LiteSpeed Cache plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'comment' parameter in all versions up to, and including, 7.9.1 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 vulnerability is only exploitable when the HTML Minify option (O_OPTM_HTML_MIN) is enabled and a companion plugin renders stored comment content into a raw-text context such as a JSON-LD script block on the same page.	5.4	More Deta
CVE-2026-117623	Jenkins 2.587 and earlier, LTS 2.580.1 and earlier does not escape the text shown in the tooltips of breadcrumb bar overflow menu entries, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Overall/Read permission.	5.4	More Deta
CVE-2026-76058	The PayPal Brasil para WooCommerce plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.7.8. 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 disable or enable the PayPal Brasil BCDC payment gateway and overwrite its WooCommerce gateway settings, removing PayPal from checkout for all customers.	5.3	More Deta
CVE-2026-119545	Forgejo through 15.0.11, 16.0.0 through 16.0.7, and 17.0.0 through 17.0.1 contains a server-side request forgery vulnerability that allows unauthenticated attackers to make the server issue requests by submitting arbitrary OpenID identifier URLs. Attackers can POST crafted identifiers to /user/login/openid to trigger blind discovery GET requests to loopback, cloud metadata, and internal addresses for port scanning and probing.	5.3	More Deta
CVE-2026-119131	Wasmtime 46.0.0 before 48.0.6 and 49.0.0 before 49.0.3 contains a denial of service vulnerability in wasmtime-wasi-http that lets guests crash the host by sending long request URLs. Guests can use set-path-with-query with a '?' after byte 65535, overflowing a u16 index in the http crate and triggering a host panic.	5.3	More Deta
CVE-2026-103391	An Out-of-bounds Write vulnerability in the SSR TCP proxy/optimization path in Juniper Networks Session Smart Router allows an attacker to corrupt forwarded packet data and potentially cause a data-plane crash via a transit TCP packet with a crafted TCP option length.	5.3	More Deta
CVE-2026-2839	The Advanced Custom Fields: Extended plugin for WordPress is vulnerable to unauthorized access of data and triggering of server-side actions in all versions up to, and including, 0.9.2.7. This is due to multiple AJAX handlers registered for unauthenticated users (`wp_ajax_nopriv_*`) that fail to implement proper `current_user_can()` authorization checks. While these handlers use ACF's `acf_verify_ajax()` function to validate cryptographic nonces, the `acf_nonce` values are generated for guest users and publicly exposed in the page source of any frontend page utilizing an ACF form. This makes it possible for unauthenticated attackers to extract the guest nonce and bypass WordPress visibility permissions, leading to the unauthorized disclosure of post titles and internal Flexible Content layout structures. The vulnerability was partially patched in version 0.9.2.4.	5.3	More Deta
CVE-			

2026-115601	Missing Authorization vulnerability in WP Desk Custom Price for WooCommerce custom-price-for-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Custom Price for WooCommerce: from n/a through 1.1.29.	5.3	More Deta
CVE-2026-62860	Picsou is a self-hosted personal finance dashboard. In the affected login implementation, the `/api/auth/login` endpoint reveals whether a username exists through a timing discrepancy. In `backend/src/main/java/com/picsou/controller/AuthController.java`, `AuthController.login()` throws `BadCredentialsException` immediately for an unknown username, before `passwordEncoder.matches(...)`, whereas an existing username with an incorrect password incurs the `bcrypt` comparison cost. Both cases return the same generic `HTTP 401` response, but repeated latency measurements disclose valid usernames without credentials. Login rate limiting, a small user population, and deployments inaccessible from outside the local network limit practical exposure; the weakness does not itself read or modify account data, though enumerated usernames can assist credential stuffing or brute-force attacks. This issue is fixed in repository release 1.0.8.	5.3	More Deta
CVE-2026-114181	Missing Authorization vulnerability in Magepeople inc. Taxi Booking Manager for WooCommerce ecab-taxi-booking-manager allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Taxi Booking Manager for WooCommerce: from n/a through 2.1.6.	5.3	More Deta
CVE-2026-119364	ProFTPD through 1.3.9e and 1.3.10rc1 through 1.3.10rc4 contains a link-following vulnerability in mod_copy that allows authenticated FTP users to bypass Limit WRITE restrictions via symlinks. Attackers can place a symlink in a writable directory and use SITE COPY or SITE CPTO to overwrite files in write-denied locations.	5.3	More Deta
CVE-2026-54871	Missing Authorization vulnerability in Mamunur Rashid ShopBuilder – Elementor WooCommerce Builder Addons shopbuilder allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects ShopBuilder – Elementor WooCommerce Builder Addons: from n/a through 3.4.2.	5.3	More Deta
CVE-2026-90871	Improper limitation of a pathname to a restricted directory in Progress Software WS_FTP Server versions prior to 2024.0.7 and 2025.0.4 on Windows could allow an unauthenticated attacker to affect files outside the intended directory.	5.3	More Deta
CVE-2026-48200	Insertion of Sensitive Information Into Sent Data vulnerability in Barn2 Plugins Document Library Lite document-library-lite allows Retrieve Embedded Sensitive Data.This issue affects Document Library Lite: from n/a through 1.3.0.	5.3	More Deta
CVE-2026-97073	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 Deta
CVE-2026-119141	Wasmtime 46.0.0 before 48.0.6 and 49.0.0 before 49.0.3 contains a denial of service vulnerability that allows malicious Wasm modules to panic the host because the may_leave flag is not cleared during realloc. Attackers can call into the host from realloc while lowering stream or future results, such as cancelling the active read or re-waiting a waitable-set, crashing the host.	5.3	More Deta
CVE-2026-119137	Wasmtime 42.0.0 before 48.0.6 and 49.0.0 before 49.0.3 contains a stack overflow vulnerability that allows guests to crash the host through recursive type drops. Guests can define a long chain of recursive types so that removing the top-level type triggers unbounded recursive drops, exhausting the host stack.	5.3	More Deta
CVE-2026-107046	A Server-Side Request Forgery (SSRF) in the url/title/author/coverUrl component of FocusPodcast versionCode 70allows attackers to scan internal resources via supplying a crafted URL.	5.3	More Deta
CVE-2026-48202	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Brave Brave brave-popup-builder allows Code Injection.This issue affects Brave: from n/a through 0.8.8.	5.3	More Deta
CVE-2026-107262	Cross-Site Request Forgery (CSRF) vulnerability in Drupal Advanced Filesystem allows Cross Site Request Forgery. This issue affects Advanced Filesystem versions: from 0.0.0 to 1.0.28.	5.3	More Deta
CVE-2026-119342	Stirling-PDF is a locally hosted web application that facilitates various operations on PDF files. From 2.13.1 until 2.13.2, the POST /api/v1/convert/svg/pdf endpoint renders attacker-supplied SVG through Apache Batik, and a scheme-less root-relative image reference bypasses SvgSanitizer.isExternalUrl() before Batik resolves it against the file:///input.svg document base as a same-origin local file. The convert() and addSvgAsPage() paths in app/core/src/main/java/stirling/software/SPDF/utils/SvgToPdf.java can then render image-decodable server files into the returned PDF when sanitization is enabled, including without authentication on login-disabled deployments or with non-admin access when login is enabled. The issue discloses PNG, JPG, GIF, or SVG content and provides an existence oracle only for image-decodable paths; plain text, binary files, directories, XInclude text, external entities, explicit file URLs, and tested HTTP references are not disclosed through this mechanism. This issue is fixed in version 2.13.2.	5.3	More Deta
CVE-2026-119564	Plausible Analytics Community Edition through 3.2.1 contains an information exposure vulnerability that allows site editors to obtain pending invitation and ownership-transfer IDs from the settings/people page. Attackers can register with the invitee's email using the exposed ID and accept it, gaining the invited role or taking site ownership.	5.3	More Deta
CVE-2026-48884	Missing Authorization vulnerability in weDevs WP User Frontend wp-user-frontend allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP User Frontend: from n/a through 4.3.13.	5.3	More Deta
CVE-2026-54853	Missing Authorization vulnerability in Cozmoslabs Profile Builder profile-builder allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Profile Builder: from n/a through 4.0.5.	5.3	More Deta
CVE-2026-110508	The Essential Addons for Elementor WordPress plugin before 6.8.7 does not apply its administrator approval requirement to accounts registered through its email one-time-password flow, which could allow unauthenticated users to register and log in without being approved by an administrator when both features are enabled.	5.3	More Deta
CVE-2026-118101	The BuddyForms WordPress plugin before 2.10.1 does not verify that a user editing an existing entry is the author of the target post, allowing users who have been granted edit access to a form, as low as Subscriber, to overwrite the title, content and status of any other user's posts or pages, including those of administrators.	5.3	More Deta
CVE-2026-27063	Missing Authorization vulnerability in Kit Kit (formerly ConvertKit) convertkit allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Kit (formerly ConvertKit): from n/a through 3.4.7.	5.3	More Deta

CVE-2026-25450	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.	5.3	More Deta
CVE-2026-106648	The Royal Elementor Addons WordPress plugin before 1.7.1070 does not validate submitted form field values before substituting them into the recipient addresses of its form notification emails, allowing unauthenticated attackers to replace the recipient list and relay attacker-composed email from the site's own domain when a recipient field is configured to echo a submitted value.	5.3	More Deta
CVE-2026-118100	The BuddyForms WordPress plugin before 2.10.3 does not check that the requester is allowed to manage a form before exporting its configuration, allowing unauthenticated users to download any form's stored settings, including notification recipient email addresses and reCAPTCHA secret keys that are not shown on the public form.	5.3	More Deta
CVE-2026-118091	Missing Authorization vulnerability in WPFunnels Team WPFunnels wpfunnels allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WPFunnels: from n/a through 3.13.5.	5.3	More Deta
CVE-2026-39782	Missing Authorization vulnerability in Kaliforms Kali Forms kali-forms allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Kali Forms: from n/a through 2.4.27.	5.3	More Deta
CVE-2026-118088	Missing Authorization vulnerability in WPFunnels Team WPFunnels wpfunnels allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WPFunnels: from n/a through 3.13.5.	5.3	More Deta
CVE-2026-107267	Missing Authorization vulnerability in Drupal DKAN allows Forceful Browsing. This issue affects DKAN versions: from 0.0.0 to 4.0.4, from 4.1.0 to 4.1.5.	5.3	More Deta
CVE-2026-116856	Missing Authorization vulnerability in WP Desk Flexible Quantity – Measurement Price Calculator for WooCommerce flexible-quantity-measurement-price-calculator-for-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Flexible Quantity – Measurement Price Calculator for WooCommerce: from n/a through 2.3.24.	5.3	More Deta
CVE-2026-103330	The Sadad QA Payment WordPress plugin through 1.28 does not correctly verify the authenticity of incoming payment notifications, as the verification is keyed on a merchant secret that is empty by default and the rest of the signed data is attacker-controlled, allowing unauthenticated attackers to forge a valid confirmation and mark orders as paid without payment.	5.3	More Deta
CVE-2026-54852	Missing Authorization vulnerability in miniOrange Page Restriction WordPress (WP) page-and-post-restriction allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Page Restriction WordPress (WP): from n/a through 1.6.1.	5.3	More Deta
CVE-2026-90870	A missing release of backend receiver sessions in the Ad Hoc Transfer component of Progress Software WS_FTP Server versions prior to 2024.0.7 and 2025.0.4 on Windows could lead to server resource exhaustion and service degradation.	5.3	More Deta
CVE-2026-103313	The BitPay Gateway for WooCommerce WordPress plugin through 4.1.3 does not bind the payment provider's transaction confirmation to the order it completes, nor verify the confirmed amount, allowing an unauthenticated attacker who holds a single genuine low-value transaction to mark arbitrary higher-value orders as paid.	5.3	More Deta
CVE-2026-116846	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 2.9.26.	5.3	More Deta
CVE-2026-92665	Dell PowerProtect Data Domain, Feature Release versions 7.7.1.0 through 8.8, LTS2024 release versions 7.13.1.0 through 7.13.1.80, LTS2025 release versions 8.3.1.0 through 8.3.1.40, LTS2026 release versions 8.6.1.0 through 8.6.1.20, contain an Allocation of Resources Without Limits or Throttling vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Denial of service.	5.3	More Deta
CVE-2026-86388	Dell PowerProtect Data Domain, Feature Release versions 7.7.1.0 through 8.8, LTS2024 release versions 7.13.1.0 through 7.13.1.80, LTS2025 release versions 8.3.1.0 through 8.3.1.40, LTS2026 release versions 8.6.1.0 through 8.6.1.20, contain an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Filesystem access for attacker.	5.3	More Deta
CVE-2026-116387	Missing Authorization vulnerability in Brainstorm Force SureForms sureforms allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects SureForms: from n/a through 2.12.9.	5.3	More Deta
CVE-2026-63115	ActivityPub is a multi-tenant ActivityPub server for Ghost, built with Fedify. From 1.0.0 until 1.2.6, the `Undo` handler allows a remote federated server to cause the service to act on a `follow` or `repost` as though the activity came from a different account. This permits removal of an existing `follow` relationship or `repost` belonging to another account without that account's involvement. No private data is exposed and content is not modified; the affected relationships can be re-established. Services proxying to Ghost's hosted ActivityPub server have already been updated, while self-hosted services require an updated image and redeployment. This issue is fixed in version 1.2.6.	5.3	More Deta
CVE-2026-119423	OPNsense core before 26.7.8 contains a log injection vulnerability that allows unauthenticated attackers to plant victim IP addresses in the lockout_handler by submitting crafted WebGUI login usernames. Attackers can submit usernames like 'Invalid user <victim-ip>' repeatedly to add the victim to the sshlockout table, blocking SSH and WebGUI access and killing its pf states.	5.3	More Deta
CVE-2026-119122	Crawl4AI before 0.9.5 contains a blind server-side request forgery vulnerability in the Docker server that allows API clients to bypass the egress proxy by enabling check_cache_freshness. Attackers can cache a controlled URL, then trigger CacheValidator to follow 302 redirects or DNS rebinding to internal and cloud-metadata addresses for port and service discovery.	5.3	More Deta
CVE-2026-103390	An Out-of-Bounds Read vulnerability in the HttpParser component in Juniper Networks Session Smart Router and Session Smart Conductor allows an attacker to cause a denial of service via a specially crafted HTTP request.	5.3	More Deta
CVE-2026-119711	PipesHub before 0.10.0 contains a rate limit bypass vulnerability in getClientIp() that allows unauthenticated attackers to evade per-IP throttling by spoofing X-Forwarded-For or X-Real-IP headers. Attackers can rotate header values to obtain fresh rate-limit buckets on authentication endpoints, enabling password spraying and OTP or password-reset email flooding.	5.3	More Deta
CVE-	The Royal Addons for Elementor WordPress plugin before 1.7.1070 does not verify that a requested post is publicly viewable before returning its content via an unauthenticated AJAX action, relying only on the published status and not on the post type's visibility, allowing unauthenticated		More

2026-107100	users to disclose the content of posts stored in non-public post types, for example captured contact-form submissions containing names, email addresses and messages.	5.3	Deta
CVE-2026-106002	The Court Reservation WordPress plugin before 1.12.4 does not perform any authorisation or nonce verification on one of its challenge-management actions, allowing unauthenticated users to delete arbitrary tournament-ladder challenge records, along with the linked court-booking event when one was scheduled.	5.3	More Deta
CVE-2026-115255	The WP Roster WordPress plugin before 2.35 does not perform any capability or nonce checks on one of its AJAX actions, allowing unauthenticated attackers to delete the WordPress user accounts of roster members.	5.3	More Deta
CVE-2026-107868	Unauthenticated Bypass Vulnerability in YITH WooCommerce Product Add-Ons <= 4.34.0 versions.	5.3	More Deta
CVE-2026-117349	Bitcoin Core prior to 29.5, 30.4, 31.2 and 32.1 is vulnerable to an OOM issue.	5.3	More Deta
CVE-2026-40063	A information disclosure vulnerability exists in the /nodered/fuxa/scripts functionality of FUXA (version(s): 1.3.2-2809). A specially crafted HTTP request can lead to an information leak. An attacker can make an unauthenticated HTTP request to trigger this vulnerability.	5.3	More Deta
CVE-2026-118275	A vulnerability was found in a2ui-project a2ui up to 0.10.6. This affects the function DataContext.resolveSignal of the file renderers/web_core/src/v0_9/rendering/data-context.ts of the component Resolver. The manipulation results in resource consumption. The attack can be launched remotely. The exploit has been made public and could be used. The patch is identified as c76e17272e52c12c6dcf68905b1df978c39e9aa5. It is advisable to implement a patch to correct this issue.	5.3	More Deta
CVE-2026-114173	The Ortto plugin for WordPress before 1.0.25 did not filter the WooCommerce product data it embedded in public storefront pages. An unauthenticated threat actor could read product passwords and private product metadata from an affected store.	5.3	More Deta
CVE-2026-106003	The Court Reservation WordPress plugin before 1.12.4 does not perform any authorization, authentication or nonce validation on one of its AJAX actions, allowing unauthenticated users to add or delete reservation types in the Court Reservation WordPress plugin before 1.12.4's configuration.	5.3	More Deta
CVE-2026-118590	A security vulnerability has been detected in nipy nibabel up to 5.4.2. The affected element is the function array_from_file of the file nibabel/volumeutils.py of the component Header Handler. The manipulation leads to uncontrolled memory allocation. The attack is possible to be carried out remotely. The pull request to fix this issue awaits acceptance.	5.3	More Deta
CVE-2026-116860	Missing Authorization vulnerability in Arraytics Timetics timetics allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Timetics: from n/a through 1.0.65.	5.3	More Deta
CVE-2026-118589	A weakness has been identified in nschloe meshio up to 5.3.5. Impacted is an unknown function of the file meshio/_vtk_42.py of the component VTK Reader. Executing a manipulation of the argument DIMENSIONS can lead to uncontrolled memory allocation. The attack can be executed remotely. The project was informed of the problem early through an issue report but has not responded yet.	5.3	More Deta
CVE-2026-118586	A security flaw has been discovered in dfm feedfinder2 up to 0.0.4. This issue affects the function find_feeds of the file feedfinder2.py. Performing a manipulation results in server-side request forgery. Remote exploitation of the attack is possible. The project was informed of the problem early through an issue report but has not responded yet.	5.3	More Deta
CVE-2026-120046	Nezha 2.0.0 before 2.4.0 contains a NULL pointer dereference vulnerability in ServiceSentinel.loadTodayStats that allows authenticated users to crash the dashboard by deleting a service. Attackers can delete their own service via POST /api/v1/batch-delete/service, leaving orphaned service_histories rows that crash the non-TSDB dashboard on its next startup until removed manually.	5.3	More Deta
CVE-2026-107097	The Royal Addons for Elementor WordPress plugin before 1.7.1070 does not perform any authorization check before using the site owner's stored Mailchimp credential to add subscriber records to an audience chosen by the request, allowing unauthenticated attackers to inject arbitrary email addresses and contact details into the site owner's Mailchimp account as confirmed subscribers.	5.3	More Deta
CVE-2026-118754	Dolibarr ERP CRM before 24.0.2 contains a missing authorization vulnerability in htdocs/public/recruitment/view.php that allows unauthenticated attackers to view unpublished draft job positions. Attackers can enumerate sequential provisional references via the ref parameter to read titles, descriptions, salary budgets, and recruiter names and emails.	5.3	More Deta
CVE-2026-110030	The Hide Price Until Login WordPress plugin before 1.1.2 does not restrict a guest-registration handler and does not honour the site's user-registration setting, allowing anyone to create a WordPress account and obtain a logged-in session even when registration is disabled.	5.3	More Deta
CVE-2026-91153	The Everest Forms – Contact Form, Payment Form, Quiz, Survey & Custom Form Builder with AI plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.6.2 via the process. This makes it possible for unauthenticated attackers to extract arbitrary WordPress post meta values — including license keys, API tokens, SMTP credentials, and Stripe or AWS secrets stored on any post type — via form submission notification emails or stored entries. The submission nonce is publicly rendered in every embedded form and can additionally be minted anonymously via the nopriv everest_forms_get_form_update_nonce action, meaning no account or prior authentication of any kind is required to complete the exploit.	5.3	More Deta
CVE-2026-119368	Missing Authorization vulnerability in Liquid Web / StellarWP The Events Calendar the-events-calendar allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects The Events Calendar: from n/a through 6.18.2.	5.3	More Deta
CVE-2026-115302	The Contact Form by Supsystic WordPress plugin before 1.11.1 does not restrict access to an AJAX action that deletes stored form statistics records, allowing unauthenticated attackers to delete arbitrary statistics entries.	5.3	More Deta
CVE-2026-117688	A flaw was found in the client registration component of Keycloak, an open-source identity and access management solution. When a vault provider is used to store sensitive information, an authenticated client owner can use a specially crafted reference to trick the system into revealing secrets. By updating a client secret to point to a vault entry and then requesting the client configuration, the owner can see the secret value in plain text. This could lead to the exposure of sensitive credentials that the user should not be able to access.	5.3	More Deta

CVE-2026-105997	The Booking Package WordPress plugin before 1.7.33 does not restrict who can trigger its booking verification-code emails nor bind the recipient to server-side state, allowing unauthenticated users to make the site send templated verification-code emails to arbitrary recipients.	5.3	More Deta
CVE-2026-93536	A use after free caused by missing lifecycle management of gesture sprites in GestureBuildSprite() in X.Org X Server before 21.1.25 and XWayland before 24.1.14 could be used by authenticated X clients to crash the X server or potentially execute code.	5.3	More Deta
CVE-2026-103382	The Casso Flow WordPress plugin before 4.2.0 does not properly authenticate incoming bank-transfer payment notifications, as the token used to verify them is empty on a default installation, allowing unauthenticated attackers to forge a notification and mark any pending WooCommerce order as paid, regardless of its payment method.	5.3	More Deta
CVE-2026-78396	The Link Library WordPress plugin before 7.10.0 does not verify that a requested link belongs to the settings set whose display template is used to render it, allowing unauthenticated users to disclose the telephone number, e-mail address and submitter name stored with links that the settings set is configured not to display.	5.3	More Deta
CVE-2026-78395	The Link Library WordPress plugin before 7.10.0 does not re-check the selected library's own login requirement when processing its front-end link submission, allowing unauthenticated users to submit links to a library configured to require login by reusing a form token obtained from another library that does not.	5.3	More Deta
CVE-2026-7003	WIT SynApps Runtime through 1.4.11 contains a hardcoded credentials vulnerability that allows unauthenticated attackers to recover static OAuth clientId and clientSecret values embedded in JavaScript delivered to the frontend, such as in parameters.js. Attackers can extract these exposed application credentials to reproduce the application portion of the REDY authentication flow at the /web/api/v1/auth/token endpoint, undermining confidential-client assurance for the OAuth implementation.	5.3	More Deta
CVE-2026-119482	Missing Authorization vulnerability in Crocoblock JetFormBuilder jetformbuilder allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects JetFormBuilder: from n/a through 3.6.7.1.	5.3	More Deta
CVE-2026-115282	The Recipe Card Blocks Lite WordPress plugin before 3.6.4 does not perform an authorization check before rendering posts through its recipe print feature, allowing unauthenticated users to disclose the title, ID and recipe content of unpublished posts, including drafts, pending, private and password-protected posts, that contain a recipe card block. Its optional "print only published posts" protection does not prevent this, because the status check is applied to a different post than the one ultimately rendered.	5.3	More Deta
CVE-2026-103372	The Payconiq WordPress plugin through 1.0.4 does not check that a visitor is allowed to see an order before returning its confirmation link, allowing unauthenticated users to obtain any paid order's key and, for recent guest orders, view the customer's personal details.	5.3	More Deta
CVE-2026-119763	changelog.com before commit 7b35e829 contains a missing authorization vulnerability that allows unauthenticated attackers to read unpublished content via preview routes in PostController, NewsIssueController and NewsItemController. Attackers can enumerate hashid post IDs, sequential newsletter slugs and integer news IDs against preview endpoints to read draft posts, unsent newsletters and declined news items.	5.3	More Deta
CVE-2026-103331	The UniPAY Payment Gateway For WooCommerce WordPress plugin through 2.3 does not properly verify the authenticity of payment notifications, as their signature is checked against a merchant secret that is empty by default, allowing unauthenticated attackers to forge a valid notification and mark arbitrary orders as paid.	5.3	More Deta
CVE-2026-114270	The GeoDirectory WordPress plugin before 2.8.197 does not honour post password protection when rendering a listing, allowing unauthenticated users to disclose the content and custom fields of published listings that are protected by a post password.	5.3	More Deta
CVE-2026-110509	The Essential Addons for Elementor WordPress plugin before 6.8.7 does not restrict the post type or meta query an unauthenticated visitor can pass to its pagination endpoint, which could allow them to read content of non-public post types and recover the values of private custom fields on published posts.	5.3	More Deta
CVE-2026-27401	Missing Authorization vulnerability in YITH YITH PayPal Express Checkout for WooCommerce yith-paypal-express-checkout-for-woocommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects YITH PayPal Express Checkout for WooCommerce: from n/a through 1.62.0.	5.3	More Deta
CVE-2026-52710	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in ithemelandco GIFTiT – Free Gifts for WooCommerce ithemeland-free-gifts-for-woo allows Code Injection.This issue affects GIFTiT – Free Gifts for WooCommerce: from n/a through 4.5.	5.3	More Deta
CVE-2026-118663	@hono/node-server allows running the Hono application on Node.js. From 1.19.10 until 2.1.3, serveStatic decodes a request path a second time after Hono has already decoded it for routing, so a malformed percent-encoded sequence can make route middleware evaluate an encoded path while static file resolution uses a different directory. An unauthenticated attacker can bypass middleware mounted on a protected static prefix and read a file inside the configured static root, although the flaw does not permit traversal outside that root. This issue is fixed in version 2.1.3.	5.3	More Deta
CVE-2026-39741	Missing Authorization vulnerability in RelyWP Simple Cloudflare Turnstile simple-cloudflare-turnstile allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Simple Cloudflare Turnstile: from n/a through 1.44.0.	5.3	More Deta
CVE-2026-62057	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Fahim Reza Divi Contact Form 7 cf7-styler-for-divi allows Code Injection.This issue affects Divi Contact Form 7: from n/a through 4.1.0.	5.3	More Deta
CVE-2026-62056	Missing Authorization vulnerability in WP ManageNinja LLC Fluent CRM fluent-crm allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Fluent CRM: from n/a through 3.2.6.	5.3	More Deta
CVE-2026-118093	Missing Authorization vulnerability in WPFunnels Team Product Feed Manager best-woocommerce-feed allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Product Feed Manager: from n/a through 7.14.1.	5.3	More Deta
CVE-2026-93011	A flaw was found in dnsmasq. After a reduction of internal domain-name buffer sizes, the DNSSEC validator can write a few bytes past a name buffer when converting names to and from DNS wire format. An attacker who can cause the server to validate a crafted DNSSEC response may overwrite a small amount of adjacent heap metadata. DNSSEC support is not compiled in by default and must also be enabled at runtime.	5.3	More Deta
CVE-2026-	Missing Authorization vulnerability in Arraytics Booktics booktics allows Exploiting Incorrectly Configured Access Control Security Levels.This issue	5.3	More

62122	affects Booktics: from n/a through 1.0.31.		Deta
CVE-2026-118653	Echo is a Go web framework. From 4.0.0 until 5.1.0, Context.RealIP falls back to client-supplied X-Forwarded-For or X-Real-IP values when Echo.IPExtractor is unset, and the default RateLimiter uses that result as its client identifier. A remote attacker can rotate arbitrary forwarded-address values to obtain new rate-limit buckets and bypass IP-based throttling used for controls such as brute-force or request-volume protection. This issue is fixed in Echo v5.1.0.	5.3	More Deta
CVE-2026-118651	Echo is a Go web framework. From 4.0.0 until 5.4.0, the Proxy middleware can preserve an attacker-supplied X-Real-IP header and forward it to an upstream service when Echo.IPExtractor is not configured. A remote client can therefore make upstream services receive a spoofed client address, undermining IP-based access controls, rate limiting, audit logging, or geographic restrictions that trust Echo's forwarded identity. This issue is fixed in Echo 5.4.0.	5.3	More Deta
CVE-2026-118266	Echo is a Go web framework. Prior to 4.16.0 and 5.4.0, Echo's MethodOverride middleware accepts a safe HTTP method as the override target for a POST request. When MethodOverride is registered before CSRF in the post-routing middleware chain, route selection retains the original state-changing POST handler but the override changes the method before CSRF evaluates it, causing both token validation and Sec-Fetch-Site checks to be skipped. A cross-site exploit requires an authenticated victim and an override value that a browser-submitted request can control, such as the form getter used by the advisory reproducer; the default X-HTTP-Method-Override header getter is not settable by a cross-site form. This issue is fixed in 4.16.0 and 5.4.0.	5.3	More Deta
CVE-2026-119479	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 3.6.7.1.	5.3	More Deta
CVE-2026-119699	WPGraphQL Smart Cache before 2.3.3 contains an uncontrolled resource consumption vulnerability that allows unauthenticated attackers to persist unlimited query documents via the Automatic Persisted Query handler. Attackers can send distinct queries with matching SHA-256 queryId values, including batched operations, to grow the wp_posts table without bound and degrade database performance.	5.3	More Deta
CVE-2026-119569	Parse Server before 8.6.108 and 9.0.0 before 9.10.5-alpha.9 contains a prototype pollution vulnerability because user-controlled keys are expanded into objects without own-property checks. Clients with class write access can send dot notation field keys or ACL entry names matching built-in object members to corrupt built-in functions, causing all requests to fail until server restart.	5.3	More Deta
CVE-2026-92086	The MW WP Form plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 5.1.7 via the 'post_id' parameter. This makes it possible for unauthenticated attackers to extract personally identifiable information from other users' form inquiry records, including submitted names, email addresses, and free-text message bodies, by enumerating sequential post IDs. Exploitation requires the targeted form to have the querystring setting enabled, but this is a standard documented feature of the plugin.	5.3	More Deta
CVE-2026-119700	WPGraphQL before 2.24.2 contains an information disclosure vulnerability that allows unauthenticated attackers to determine object existence through distinct error responses. Attackers can iterate IDs against deleteMediaItem, updateMediaItem, deleteComment and updateComment mutations to discover hidden draft, private, trashed posts, custom post types, and unapproved comments.	5.3	More Deta
CVE-2026-119701	WPGraphQL before 2.24.1 contains a missing rate limiting vulnerability that allows unauthenticated attackers to flood password reset emails by aliasing the sendPasswordResetEmail mutation. Attackers can send one HTTP request with many aliases, bypassing batch_limit, to exhaust mail provider quota and repeatedly rotate reset keys, blocking legitimate password recovery.	5.3	More Deta
CVE-2026-116402	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Brainstorm Force SureForms sureforms allows Code Injection.This issue affects SureForms: from n/a through 2.12.9.	5.3	More Deta
CVE-2026-119705	SerpBear before 3.1.1 contains a missing authentication vulnerability in pages/api/notify.ts that allows remote unauthenticated attackers to trigger notification emails because verifyUser() is never called. Attackers can repeatedly POST to /api/notify, optionally with a domain parameter, to exhaust SMTP rate limits, trigger provider abuse flags and flood recipients.	5.3	More Deta
CVE-2026-118376	WeKnora before 0.8.2 contains a server-side request forgery vulnerability in isRestrictedIP() that misclassifies NAT64-prefixed IPv6 addresses as public. Authenticated attackers can supply URLs resolving to NAT64 encodings of internal addresses via web_fetch or URL-based knowledge import to reach internal services or cloud metadata endpoints.	5.3	More Deta
CVE-2026-118265	Echo is a Go web framework. From 5.0.0 until 5.4.1, Echo v5's ExtractIPFromRealIPHeader validates whether the client-supplied X-Real-IP value belongs to a trusted range instead of validating the direct network peer. A client reaching Echo directly, or through a proxy that preserves the header, can supply a loopback or private address and have Context.RealIP return that spoofed identity. Applications using the extractor for IP allowlists, rate limiting, audit logs, or forwarding headers can consequently trust an attacker-controlled address; the default direct extractor and Echo v4 are unaffected. This issue is fixed in 5.4.1.	5.3	More Deta
CVE-2026-118259	opentelemetry-java is the Java implementation of the OpenTelemetry API for recording telemetry, and SDK for managing telemetry recorded by the API. Prior to 1.67.0, W3CTraceContextPropagator.extract() uses regex delimiter processing that can exhibit quadratic backtracking while parsing tracestate headers containing long runs of spaces or tabs without a following comma. An unauthenticated attacker whose headers reach extraction can repeatedly block request or event-loop threads and cause excessive CPU consumption, with practical impact bounded by ingress header-size limits, proxy configuration, and threading. This issue is fixed in version 1.67.0.	5.3	More Deta
CVE-2026-119053	lwIP 2.0.0 through 2.2.1 built with the SNMP agent contains an out-of-bounds read vulnerability in snmp_pbuf_stream_writeto() that bounds copies by pbuf->len instead of remaining bytes. Remote unauthenticated attackers knowing the read community can send fragmented SNMP requests to receive adjacent receive-buffer or pool memory echoed in responses.	5.3	More Deta
CVE-2026-25467	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in ThemeGrill User Registration user-registration allows Code Injection.This issue affects User Registration: from n/a through 5.3.0.	5.3	More Deta
CVE-2026-93007	A flaw was found in dnsmasq. The TCP DNS service uses a small fixed pool of child processes and does not set a receive timeout on client connections. A remote attacker can open idle TCP connections to port 53 and occupy the entire pool, preventing new TCP DNS connections and DNSSEC validation that requires TCP fallback. UDP DNS resolution continues, and occupied slots are released after a fixed lifetime.	5.3	More Deta
CVE-2026-88941	Kaspersky has fixed a vulnerability in the Network Agent for Windows module of Kaspersky Security Center. The vulnerability could potentially cause the Network Agent module of Kaspersky Security Center to malfunction. There are no evidence of the vulnerability exploitation in-the-wild.	5.2	More Deta
CVE-2026-107036	Insecure permissions in Mission Control / AIMSICD versionCode 2026080501 allows unauthorized attackers to invoke an exported component, impacting the tracker blocker mechanism of the application.	5.1	More Deta

CVE-2026-50000	SecureDrop is an open-source whistleblower submission system that media organizations can use to securely accept documents from, and communicate with anonymous sources. From 2.5.0 until 2.16.0, the `Journalist Interface` can accept an `API session` token against the `web UI` because its `SessionInterface` keeps a mutable session key prefix that changes with each request and persists across requests. API and web sessions were separated in `Redis` starting in version 2.5.0, but prefix corruption confuses those session namespaces. An attacker who already has access to the secret `Journalist Interface` onion address, the required authentication access and a recent nonexpired `API session` token can reuse that token against the `web UI` until its natural expiry, at most eight hours. The corrupted prefix can also prevent logout from deleting the correct `Redis` session, although normal expiry still applies. A compromised journalist can access encrypted submissions and perform broad actions on source submissions, but this issue does not expose plaintext submissions or affect the running system's availability. This issue is fixed in version 2.16.0.	5.0	More Deta
CVE-2026-102590	IBM Langflow OSS 1.0.0 through 1.12.3 could allow a remote authenticated attacker to obtain sensitive information due to a server-side request forgery vulnerability.	5.0	More Deta
CVE-2026-119657	FilePress through 3.0.1 contains a missing authorization vulnerability in dzz/pichome/library that allows authenticated users to manage other libraries' folders because checkuserperm_by_uid only checks membership of any library. Attackers who know another library's appid or folder id can invoke folder.php operations like deletefolder and rename, or rightdata.php getfolderdata, to delete, modify, or read foreign folders.	5.0	More Deta
CVE-2026-115604	Subscriber Arbitrary File Deletion in SureDash <= 1.12.3 versions.	5.0	More Deta
CVE-2026-59396	A denial-of-service vulnerability exists in UAA's private_key_jwt client-authentication mechanism. When UAA retrieves a remote JWKS URI, it caches the response. Invalid authentication attempts can trigger full deserialization of this cached data. An attacker with prerequisites (write access to clients or a compromised endpoint) can send anonymous requests that force repeated parsing of large cached objects, causing excessive CPU usage and potential Java heap exhaustion via OutOfMemoryError, resulting in service unavailability.	4.9	More Deta
CVE-2026-109216	The Meta Box – A Framework for Dynamic Websites plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'profile_background[<attacker-chosen key>]' parameter in all versions up to, and including, 5.15.2 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. Exploitability depends on a consuming plugin or theme built on Meta Box that exposes the background field to lower-privileged users and renders stored values via the rwmb_the_value()/format_single_value() pattern; the effective minimum privilege is whatever role that consumer permits, demonstrated at Subscriber level.	4.9	More Deta
CVE-2026-104739	The JS Help Desk – AI-Powered Support & Ticketing System plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the setSupportCustomImage function in all versions up to, and including, 5.0.1. This makes it possible for authenticated attackers, with administrator-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). Exploitation requires a two-step sequence: an administrator first saves a traversal-crafted value in the support_custom_img configuration field, then triggers deletion by uploading a new support custom image, at which point setSupportCustomImage() resolves and deletes the attacker-controlled path.	4.9	More Deta
CVE-2026-115259	The Photo Engine (Media Organizer & Lightroom) WordPress plugin before 6.6.0 does not have proper authorization checks when updating post data through one of its REST API routes in all versions up to, and including, 6.5.8. This makes it possible for authenticated attackers, with Author-level access and above, to modify the title, content, excerpt and other fields of arbitrary posts, pages and attachments, including those belonging to other users.	4.9	More Deta
CVE-2026-115223	The Smart Popup by Supsystic WordPress plugin before 2.0.2 does not prevent template-injection payloads from being stored in a popup text block and later evaluated by its template engine, because the filter meant to strip template delimiters runs before a decoding step that reconstructs them, allowing an authenticated administrator to execute arbitrary template expressions server-side and read PHP constants such as the site's database credentials and authentication keys.	4.9	More Deta
CVE-2026-104743	The Tainacan plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 1.3.0 via the 'tmp_file' parameter parameter. This makes it possible for authenticated attackers, with editor-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information. The poisoned importer path is persisted to the database and later triggered via a separate GET request to the /source_info endpoint, which passes the attacker-controlled path to fopen() and fgetcsv() and returns parsed file contents in the REST response.	4.9	More Deta
CVE-2026-86392	Dell PowerProtect Data Domain, Feature Release versions 7.7.1.0 through 8.8, LTS2024 release versions 7.13.1.0 through 7.13.1.80, LTS2025 release versions 8.3.1.0 through 8.3.1.40, LTS2026 release versions 8.6.1.0 through 8.6.1.20, contain a Heap-based Buffer Overflow vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Denial of service.	4.9	More Deta
CVE-2026-118169	The Hustle – Email Marketing, Lead Generation, Optins, Popups plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'content[cta_label]' parameter in all versions up to, and including, 7.8.14.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with custom-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. By default only Administrators hold the hustle_edit_module capability, but the plugin's built-in Permissions screen allows administrators to delegate this capability to lower roles including Subscriber, enabling Subscriber-level exploitation on sites where that delegation has been configured.	4.9	More Deta
CVE-2026-119132	Wasmtime from 49.0.0 before 49.0.3 contains a denial-of-service vulnerability that allows a WebAssembly guest to trigger a host panic by transcoding overlapping strings in fused adapters. Attackers can make a same-instance component-to-component call transferring a string whose source and destination alias each other, crashing the host instead of raising a trap.	4.8	More Deta
CVE-2026-103392	An Out-of-Bounds Write vulnerability in the TCP header processing in Juniper Networks Session Smart Router allows an attacker to corrupt TCP payload data and potentially cause session desynchronization via a transit TCP packet with an oversized SACK option length.	4.8	More Deta
CVE-2026-119566	Prometheus through 3.15.1 contains a credential leak vulnerability that allows attackers to capture Azure AD or Google IAM bearer tokens by redirecting remote_write requests to another host. Attackers controlling the remote-write endpoint or a redirecting server can return a 3xx to their host and replay the token, for example to write metrics to the victim's backend.	4.8	More Deta
CVE-2026-119703	xiaozhi-esp32-server through 0.9.8 contains an authentication bypass vulnerability in WebSocketServer._handle_auth that allows remote unauthenticated attackers to skip Bearer HMAC token verification by spoofing the Device-ID header. Attackers supplying an allowlisted MAC-address-shaped device identifier can open an authenticated WebSocket session, issue voice-assistant commands, exchange audio, and read that device's conversation context.	4.8	More Deta
CVE-2026-	Authentication Bypass Using an Alternate Path or Channel vulnerability in Drupal Authenticator Login Plus (2FA) allows Authentication Bypass. This issue affects Authenticator Login Plus (2FA) versions: from 0.0.0 to 1.0.1.	4.8	More Deta

107254			
CVE-2026-118767	Botan is a C++ cryptography library. From 1.11.22 until 3.13.0, Botan's Python binding converted Python strings containing U+0000 to const char* values without consistently rejecting the embedded NUL, causing bcrypt and check_bcrypt to process only the prefix before the NUL. Applications could validate a longer password but hash a shorter effective value, allowing application password-policy bypass; scrypt and argon2 are unaffected. This issue is fixed in version 3.13.0.	4.8	More Deta
CVE-2026-109236	The Customer Email Verification for WooCommerce plugin for WordPress is vulnerable to Authentication Bypass via a Predictable Email-Verification Token in all versions up to, and including, 2.8.2. This is due to the `authenticate_user_by_email_link()` function — hooked on the `wp` action and triggered by the `cusomer_email_verify` GET parameter — lacking any capability check or nonce verification, while the `secret_code` it validates is generated as `md5(email . time())` and the `verify_otp_nonce` required to trigger token issuance via the `wp_ajax_nopriv_resend_otp` handler is emitted to every front-end visitor through `wp_localize_script`. This makes it possible for unauthenticated attackers to log in as a newly created, verified WooCommerce customer bound to an arbitrary email address — or to flip an existing account's `customer_email_verified` meta to verified — fully bypassing the plugin's core email-verification control. Exploitation requires the `cev_user_log` table to contain a `password` column, which is absent from the fresh-install schema shipped in version 2.8.2 but is present on sites upgraded from an older version where that column was defined.	4.8	More Deta
CVE-2026-119201	Nuxt is an open-source web development framework for Vue.js. From 4.6.0 until 4.6.3, nuxt dev stores a generated appSecret in <buildDir>/app-secret, by default .nuxt/app-secret, within a directory allowed by Vite's server.fs configuration. A client with direct HTTP access to an exposed development server can fetch the file, use deriveSecret() to compute derived secrets such as the default useSession password, and forge session cookies accepted by that development server. The default localhost binding limits remote exposure, cross-origin browser reads are blocked, production builds and development servers with an explicitly configured appSecret are not affected. This issue is fixed in version 4.6.3.	4.8	More Deta
CVE-2026-71569	Server-Side Request Forgery (SSRF) vulnerability in Apache Camel A2A component. This issue affects Apache Camel: from 4.21.0 before 4.22.2. WebhookUrlValidator classified a push notification webhook host in two places that did not agree. A host written as an IP literal was matched against a list of string prefixes that named the IPv6 unique local range fc00::/7, while a host reached through a name was resolved and the resulting address classified with the InetAddress predicates isLoopbackAddress, isAnyLocalAddress, isLinkLocalAddress and isSiteLocalAddress. Those predicates do not cover the same ground as the prefix list: isSiteLocalAddress reports the deprecated fec0::/10 block and not the fc00::/7 unique local addresses that replaced it, and the JDK carries no predicate for them at all. The same address was therefore accepted or rejected depending on how it was written, and a webhook URL whose host name resolved into fc00::/7 passed a guard that refused the identical address given as a literal. PushNotificationDispatcher then sent the push notification to that address, together with any Authorization header carried in the same configuration, whose scheme and credentials the registering caller supplies. The webhook URL arrives as TaskPushNotificationConfig.url from the caller registering the push notification, so it is attacker-controlled, and allowLocalWebhookUrls is false by default, which is the configuration in which the guard is expected to hold. The response is not relayed back to the caller who registered the configuration, so what the gap yields is a blind outbound HTTPS request from the Camel process to an internal address the guard was written to refuse; reaching a service that way additionally requires that the name resolve into fc00::/7 in the target environment, that an HTTPS service be listening on that address, and that the TLS handshake succeed for the name being requested, which is why the severity is assessed medium. The same string pre-check was also wrong in the other direction: it matched the raw host string without first establishing that the host was an IP literal, so any name merely beginning with fc or fd, such as fcm.googleapis.com, was refused outright. Users are recommended to upgrade to version 4.23.0, which fixes the issue. If users are on the 4.22.x releases stream, then they are suggested to upgrade to 4.22.2. The 4.21.x release line reached end of life before this issue was resolved and will not receive a fix, so deployments on it must move to a supported release. Both the literal and the resolved path now classify the address from its raw bytes with one shared classifier, which recognises fc00::/7 and the shared address space 100.64.0.0/10, as well as IPv4-compatible, NAT64 (64:ff9b::/96) and 6to4 (2002::/16) addresses whose embedded IPv4 address is not globally routable. For deployments that cannot upgrade immediately, place authentication in front of the A2A push notification configuration path so that the webhook URL does not arrive from an untrusted caller, and deny egress from the Camel process to fc00::/7 at the network level; where the deployment has no need of IPv6, starting the JVM with -Djava.net.preferIPv4Stack=true removes the address class the gap turns on. Note that allowLocalWebhookUrls=false is already the default and does not by itself close the gap.	4.8	More Deta
CVE-2026-119552	Uptime Kuma through 2.5.8 contains a race condition in the Socket.IO first-run setup handler that allows unauthenticated attackers to create an additional administrator account. Attackers can send concurrent setup requests during the bcrypt hashing window to bypass the empty user table check, then modify monitors, API keys, and enable disableAuth.	4.8	More Deta
CVE-2026-119136	Wasmtime 42.0.0 before 48.0.6 and 49.0.0 before 49.0.3 contains insufficient checks in Store when mixing async-style and sync-style WebAssembly calls. Embedders re-entering WebAssembly via sync APIs from host functions called asynchronously can trigger runtime panics or unsound cross-thread movement of !Send host variables.	4.8	More Deta
CVE-2026-119135	Wasmtime 46.0.0 before 48.0.6 and 49.0.0 before 49.0.3 panics when the host reads a component model stream as a different Rust item type than it was created with, because the host-to-host read path asserts matching TypeIds instead of returning an error. Guest code can return a host-created StreamReader<U> that the embedder reads as StreamReader<T>, where both types map to the same component model type, crashing the embedding process.	4.8	More Deta
CVE-2026-119140	Wasmtime 46.0.0 before 48.0.6 and 49.0.0 before 49.0.3 contains a denial of service vulnerability that allows malicious components to panic the host via thread.yield in start functions. Attackers can supply a component whose start function calls an async-lowered import then thread.yield, causing an undisposed fiber drop that crashes embedders.	4.8	More Deta
CVE-2026-113409	The Ortto plugin for WordPress before 1.0.25 did not escape stored settings on its admin settings page, leading to stored cross-site scripting. A threat actor able to modify the plugin's configuration could execute arbitrary JavaScript in an administrator's session when they visited the impacted page.	4.8	More Deta
CVE-2013-20009	Linksys WAG200G through 1.01.06 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject scripts via the policy_name parameter in setup.cgi. Attackers can save a malicious policy name from the AccessRes.htm page that executes in administrators' browsers when viewing the Status > Wireless page.	4.8	More Deta
CVE-2026-119600	tcpflow through 1.6.1 contains an out-of-bounds read vulnerability that allows unauthenticated attackers to read process memory by sending packets with forged IP payload lengths. Attackers can inject crafted IPv4 or IPv6 TCP packets into captured traffic or pcap files to leak adjacent memory into reconstructed flow files or crash tcpflow.	4.8	More Deta
CVE-2026-119142	Wasmtime 46.0.0 before 48.0.6 and 49.0.0 before 49.0.3 contains a denial of service vulnerability where dropping the Future returned by TypedFunc::call_async can panic the host. When the guest task has not started, cleanup code searches only one location for work items and unwraps the resulting error, crashing embedders that cancel pending calls.	4.8	More Deta
CVE-2026-105619	PostgreSQL Anonymizer doesn't mask data accessed thru a security_invoker view. The problem is resolved in PostgreSQL Anonymizer 3.3.0 and later versions.	4.8	More Deta
CVE-2026-	Wasmtime 46.0.0 before 48.0.6 and 49.0.0 before 49.0.3 contains a denial of service vulnerability that allows guest code to trigger a host panic through out-of-bounds zero-length stream operations. Malicious guests can perform zero-length component model stream reads or writes with	4.8	More

119143	unvalidated addresses, causing Direct{Source,Destination}::remaining to panic and crash WASIp3 embedders.		Deta
CVE-2026-119139	Wasmtime 46.0.0 before 48.0.6 and 49.0.0 before 49.0.3 contains a leftover assertion in component::Func::call that rejects guest exports using the async ABI option. An attacker who supplies a component with an async-lifted export can crash the host process when an embedder invokes that export through Func::call.	4.8	More Deta
CVE-2026-119138	Wasmtime 46.0.0 before 48.0.6 and 49.0.0 before 49.0.3 contains a denial of service vulnerability that allows pending calls to trigger an assertion failure after a trap poisons the Store. Attackers supplying misbehaving guest code can cause a trap and let earlier calls proceed, crashing embedders that continue using the inconsistent Store.	4.8	More Deta
CVE-2026-118777	Forge (also called node-forge) is a native implementation of Transport Layer Security in JavaScript. Prior to 1.4.1, the forge.http client stored cookie names and paths from Set-Cookie response headers in ordinary JavaScript objects. A malicious server could use the cookie name __proto__ so that the attacker-controlled cookie path was written as a property on Object.prototype, or use inherited names such as constructor to modify Object. An empty cookie value could use the removal path to delete an inherited Object.prototype property. Applications using forge.http directly or through forge.xhr are affected; applications that do not use forge.http are unaffected. This issue is fixed in version 1.4.1.	4.8	More Deta
CVE-2026-119416	CakePHP through 5.4.3 contains an improper cookie domain validation vulnerability in the Http Client CookieCollection that allows malicious servers to receive and plant cookies by abusing unanchored suffix matching. Attackers controlling a host such as one ending in a victim domain suffix, or sending Set-Cookie Domain values for unrelated hosts, can steal session cookies or inject cookies into shared client cookie jars.	4.8	More Deta
CVE-2026-48164	Collabora Online is a collaborative online office suite based on LibreOffice technology. Prior to 24.04.18 and 25.04.11, the `host_session_id` query/form parameter is substituted into the `cool.html` editor page without HTML encoding, unlike parameters passed through the existing variable-encoding mechanism. An attacker who induces a victim to load a crafted URL can inject HTML and, in the absence of an effective `Content Security Policy`, execute scripts in the Collabora Online iframe's origin, exposing the session authentication token and page contents. A reverse proxy that preserves the `Content Security Policy` header sent by `coolwsd` mitigates the script-execution scenario. This issue is fixed in versions 24.04.18 and 25.04.11.	4.7	More Deta
CVE-2026-61575	AVideo is a video-sharing Platform. Prior to 8.1.0, `view/queue.php` uses `pathinfo` on the caller-controlled `fileURI` and stores its filename through `setTitle` in `encoder_queue.title` without neutralization. `fileURI` is not in the `objects/security.php` filter lists, and the `Login::canUpload()` capability needed to submit a queue entry can be self-granted using an attacker-controlled login site without legitimate encoder credentials. `view/index.php` loads `queue.json` from `view/queue.json.php` into the `#grid` jQuery Bootgrid table; its title formatter concatenates `row.title` into raw cell HTML. An attacker can therefore store an HTML title whose event handler runs in a privileged viewer's browser. `Encoder::getAll` limits nonadministrators to their own streamer's rows, so the victim must be an administrator who sees all rows or an operator on the attacker's streamer. A second `.html()` sink in the progress panel uses the same title but additionally depends on a helper script loaded from the streamer; the Bootgrid sink is reachable from encoder code alone. The script can read session-visible data and rendered streamer credentials, act with the viewer's privileges, and execute again for each qualifying viewer until the row is removed. This issue is fixed in version 8.1.0.	4.7	More Deta
CVE-2026-111031	The Welcart e-Commerce WordPress plugin before 2.12.6 does not validate a user-supplied URL before using it in a redirect, allowing unauthenticated attackers to redirect users to arbitrary external websites.	4.7	More Deta
CVE-2026-105614	PostgreSQL Anonymizer's `anon.image_blur()` function doesn't check the declared dimension of the provided image, allowing an attacker to provide a small image with enormous declared dimensions. This vulnerability can be exploited to exhaust the memory of a backend and OOM-kill it (when ovecommit is on), which results in a cluster-wide crash recovery. The problem is resolved in PostgreSQL Anonymizer 3.3.0 and later versions.	4.7	More Deta
CVE-2026-105613	PostgreSQL Anonymizer's range-based dummy functions dont constraint the range size. This vulnerability can be exploited to exhaust the memory of a backend and OOM-kill it (when ovecommit is on), which results in a cluster-wide crash recovery. The problem is resolved in PostgreSQL Anonymizer 3.3.0 and later versions.	4.7	More Deta
CVE-2026-116552	The Like Button Rating ♥ LikeBtn plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'HTTP_CLIENT_IP (Client-IP header)' parameter in all versions up to, and including, 2.6.64 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 site administrator to have disabled the default 'Be GDPR compliant' option, which would otherwise hash stored IP values and neutralize the payload. Successful exploitation additionally requires an action by an administrator — the attacker cannot trigger the vulnerability on their own.	4.7	More Deta
CVE-2026-118658	Echo is a Go web framework. Prior to 4.15.2 and 5.1.1, Context.Scheme returns values from X-Forwarded-Proto, X-Forwarded-Protocol, or X-Url-Scheme without validating that they are supported web schemes. WWWRedirect and NonWWWRedirect use that value to construct a Location header, so an attacker controlling a forwarded scheme header can cause a redirect to use an arbitrary URI scheme. Exploitation requires an affected redirect middleware and user interaction with the response; the HTTPS-specific redirect variants hardcode HTTPS and are unaffected. This issue is fixed in 4.15.2 and 5.1.1.	4.7	More Deta
CVE-2026-54162	Ember is a real-time terminal dashboard for Caddy servers with FrankenPHP support. Prior to 1.4.2, interactive TUI row formatters pass Caddy access-log fields, particularly the request URI, through the `fitCellLeft` render helper without neutralizing terminal escape or control sequences. An unauthenticated remote client can place ANSI, OSC, or CSI control bytes in an ordinary HTTP request target. Caddy JSON-escapes those bytes, `ParseLogLine` decodes them back into raw controls, and the formatters concatenate them into `View()` output reaching `os.Stdout`. When the operator views the default `Logs` tab, the terminal interprets these sequences, allowing monitoring-dashboard spoofing, clipboard hijacking through `OSC 52`, and window-title spoofing through `OSC 0/2`. This works even with a loopback-only log listener because the input arrives through normal Caddy access logs. `Certificates` and `Routes` share secondary unneutralized render sinks. The `--json`, `--once`, and daemon `--expose` modes are unaffected because they do not render an interactive terminal. Consequences depend on the terminal emulator and usually require further operator action to escalate; this is not general-purpose remote code execution. This issue is fixed in version 1.4.2.	4.7	More Deta
CVE-2026-61529	Endatix is a self-hosted form and survey management platform with a headless API. Prior to 0.7.0, the anonymous `POST /forms/{formId}/submissions` endpoint stores attacker-controlled `JsonData` after checking only that the JSON is well formed. A file object with `name`, `type` and `content` fields can contain an HTTP or HTTPS URL. When a staff member with `submissions.view` permission invokes `POST /forms/{formId}/submissions/{submissionId}/files`, `GetFilesHandler` passes the stored data to `SubmissionFileExtractor` in `src/Endatix.Infrastructure/Features/Submissions/SubmissionFileExtractor.cs`, which calls `HttpClient.GetAsync` without validating the destination URL, host or resolved IP addresses against internal address ranges. This permits stored, second-order server-side GET requests to internal services, cloud metadata, loopback and link-local addresses from the server's network position. The form must have `IsPublic` and `IsEnabled` set, and an anonymous submission must pass reCAPTCHA v3 when configured. The fetched response is placed in the staff viewer's ZIP, not returned directly to the attacker, so disclosure to the attacker is blind or indirect through observable request behavior or information exposed by the viewer. No integrity or availability impact is asserted; data: and raw-base64 `content` are decoded locally without network requests. This issue is fixed in version 0.7.0.	4.7	More Deta
CVE-	CherryTree through 1.7.2 contains a path traversal vulnerability in CtStorageXmlHelper::_create_image_from_xml that trusts unvalidated		

2026-118693	embedded-file 'filename' attributes in XML documents. Attackers can craft a .ctd, .ctz, or .ctx document with an absolute or ~/ filename and no data, so saving embeds files like ~/.ssh/id_rsa into the document.	4.7	More Deta
CVE-2026-103875	The Media Library Assistant plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'search-string' parameter in all versions up to, and including, 3.42 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. Exploitation requires the targeted site to have a publicly accessible page containing an [mla_gallery] shortcode configured with a pagination output mode and an mla_link_href template that reflects a {+request:...+} token, along with enough attachments to trigger pagination.	4.7	More Deta
CVE-2026-111498	OpenManage Enterprise, versions prior to 4.8.0, contains an Improper Resource Locking vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Protection mechanism bypass.	4.7	More Deta
CVE-2026-115277	The User Frontend WordPress plugin before 4.3.14 does not sanitise and escape some user-supplied values before reflecting them into HTML attributes in a publicly reachable AJAX response, leading to Reflected Cross-Site Scripting. The affected action is gated by an anonymous nonce that only validates for logged-out requests, so the payload executes against logged-out visitors rather than authenticated users.	4.7	More Deta
CVE-2026-110707	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 'media:group/media:description (XML element in the imported feed)' parameter in all versions up to, and including, 5.2.12 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Exploitation requires an administrator to configure a Feed-to-Post import pointing at an attacker-controlled feed URL and trigger the import via the Run Now action or setup wizard, which is the plugin's standard configuration flow.	4.7	More Deta
CVE-2026-114444	The Security Plugin, Firewall & Malware Scanner with Auto Removal WordPress plugin before 2.191 does not restrict its File System Watcher file viewer to Super Admins or to the files it legitimately tracks, allowing a non-super-admin administrator, including a subsite administrator on WordPress multisite, to read the contents of sensitive tracked files such as the main configuration file and disclose the site's authentication keys, salts and, on a standard install, database credentials.	4.4	More Deta
CVE-2026-119573	Traefik 3.7.11 before 3.7.15 contains an authorization bypass in the Kubernetes Ingress NGINX provider that skips the cross-namespace check on the auth-tls-secret annotation when a cached client authentication TLS option is reused. Users who can create Ingresses can reference another namespace's CA secret already used by another Ingress, enforcing it on their own routes and learning whether it exists, without disclosure of its contents.	4.4	More Deta
CVE-2026-118680	SiYuan 3.8.7 through 3.8.8 fails to normalize Windows GLOBALROOT device-namespace aliases, bypassing the IsSensitivePath denylist. Attackers can invoke importStdMd with a GLOBALROOT-prefixed path to copy the API token and TLS private key into the publicly served assets directory.	4.4	More Deta
CVE-2026-69446	Incorrect authorization in Microsoft Edge (Chromium-based) allows an authorized attacker to elevate privileges locally.	4.4	More Deta
CVE-2026-106484	Insufficient policy enforcement in chrome-devtools-mcp in Google Chrome on Linux prior to 1.5.0 allowed a local attacker to perform arbitrary read/write via a malicious file. (Chromium security severity: Medium)	4.4	More Deta
CVE-2026-109988	The Product Addons for Woocommerce – Product Options with Custom Fields plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'fields[section][fields][row][col][type]' parameter in all versions up to, and including, 3.1.8 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with shop manager-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	4.4	More Deta
CVE-2026-111068	The DesignSetGo plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'tagName' parameter in all versions up to, and including, 2.11.0 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. Successful exploitation requires an administrator to run the plugin's block-conversion migration ("Scan & Convert Blocks" during deactivation), which triggers the vulnerable build_group_block() function and promotes the dormant payload from a block delimiter comment into live post_content HTML. Successful exploitation additionally requires an action by an administrator — the attacker cannot trigger the vulnerability on their own.	4.4	More Deta
CVE-2026-42707	Missing Authorization vulnerability in HivePress HivePress Claim Listings hivepress-claim-listings allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects HivePress Claim Listings: from n/a through 1.1.4.	4.3	More Deta
CVE-2026-62055	Missing Authorization vulnerability in Liquid Web / StellarWP Event Tickets event-tickets allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Event Tickets: from n/a through 5.30.2.	4.3	More Deta
CVE-2026-119272	Incorrect authorization in FileSystem in Google Chrome prior to 156.0.8078.79 allowed a remote attacker leveraging social engineering to obtain sensitive information via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Deta
CVE-2026-111213	The Travelly – Tour & Travel Booking Manager for WooCommerce plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 2.3.6 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 duplicate arbitrary posts — including private, draft, and pending posts authored by Administrators and Editors — into drafts they own, thereby exposing the original post's content, excerpt, title, taxonomies, and metadata. A Contributor can harvest a valid nonce from the Duplicate row-action on their own posts list and reuse it against any victim post ID, since the nonce action is the static string 'TTBM_Admin.php' and is not bound to any specific post.	4.3	More Deta
CVE-2026-104315	IBM Langflow OSS 1.0.0 through 1.12.3 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks.	4.3	More Deta
CVE-2026-118537	A vulnerability was found in a2ui up to 0.10.4. This vulnerability affects unknown code of the file src/v0_9/basic_catalog/components/Image.js of the component Image Player/Video Player/Audio Player. Performing a manipulation of the argument url results in improper input validation. The attack may be initiated remotely. The pull request to fix this issue awaits acceptance.	4.3	More Deta
CVE-2026-	HashiCorp Nomad and Nomad Enterprise are vulnerable to cross-namespace authorization bypasses in several read-only API endpoints that may allow an authenticated user with read permissions in one namespace to view information about objects in other namespaces. This vulnerability	4.3	More

102260	(CVE-2026-102260) is fixed in Nomad Community Edition 2.1.1 and Nomad Enterprise 2.1.0, 1.11.12, and 1.10.18.		Deta
CVE-2026-111372	The AI ChatBot for WooCommerce – WoowBot plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 5.0.0. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to repeatedly trigger RAG document sync operations that issue paid embedding API calls to OpenAI, Gemini, OpenRouter, or xAI charged to the site administrator's stored API key, draining their AI API credits and causing financial loss. The wp_chatbot nonce required to reach this endpoint is emitted to every authenticated frontend visitor via wp_localize_script, making it trivially obtainable by any subscriber-level account.	4.3	More Deta
CVE-2026-119147	ProFTPD before 1.3.9e and 1.3.10rc5 contains an authorization bypass in the mod_sftp copy-file extension handler that skips Limit WRITE checks for new destination files. Authenticated SFTP users can copy any readable file to a new path in write-denied directories, creating files where uploads are forbidden.	4.3	More Deta
CVE-2026-27062	Cross-Site Request Forgery (CSRF) vulnerability in WPFunnels Team WPFunnels wpfunnels allows Cross Site Request Forgery.This issue affects WPFunnels: from n/a through 3.13.5.	4.3	More Deta
CVE-2026-111960	The Royal MCP WordPress plugin before 1.5.10 does not perform object-level or post-type authorisation checks in one of its search tools, allowing authenticated users such as a subscriber to disclose the title and content of non-public entries, including personal data stored by a companion Royal MCP WordPress plugin before 1.5.10.	4.3	More Deta
CVE-2026-118273	A flaw has been found in a2ui-project a2ui up to 0.10.6. Affected by this vulnerability is the function DataModel.set of the file renderers/web_core/src/v0_9/state/data-model.ts. Executing a manipulation can lead to resource consumption. It is possible to launch the attack remotely. The exploit has been published and may be used. This patch is called 82789191ce551f4d7a095d273773fb24bd764c9d. A patch should be applied to remediate this issue.	4.3	More Deta
CVE-2026-52708	Missing Authorization vulnerability in weDevs WP User Frontend wp-user-frontend allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP User Frontend: from n/a through 4.3.13.	4.3	More Deta
CVE-2026-90862	Improper authentication in the Web Transfer Module of Progress Software WS_FTP Server versions prior to 2024.0.7 and 2025.0.4 on Windows could allow an attacker with a user’s password to access certain files associated with that account without satisfying multi-factor authentication requirements.	4.3	More Deta
CVE-2026-76027	Information loss in CacheStorage in Google Chrome prior to 156.0.8078.79 allowed a remote attacker to obtain cross-origin data via a crafted HTML page. (Chromium security severity: High)	4.3	More Deta
CVE-2026-118667	LangGraph Python SDK is used to connect to running LangGraph API servers, manage assistants, threads and stream runs from Python applications. From langgraph-sdk 0.4.0 until 0.4.6, and from langgraph 1.2.3 until 1.2.14 when RemoteGraph v3 streaming uses an affected langgraph-sdk version, the synchronous and asynchronous v3 stream get_tree and _fetch_state helpers interpolate caller-controlled assistant_id and thread_id values into authenticated GET request paths without using _quote_path_param. Relative path segments can therefore be normalized into another readable path on the configured server while retaining authentication headers. This issue is fixed in langgraph-sdk 0.4.6 and langgraph 1.2.14.	4.3	More Deta
CVE-2026-118274	A vulnerability has been found in a2ui-project a2ui up to 0.10.6. Affected by this issue is some unknown functionality of the file renderers/web_core/src/v0_9/rendering/generic-binder.ts of the component Binder. The manipulation leads to resource consumption. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of the patch is c97f4a02d3fea33ce3e9de5cf3fd0e3b8f3a4f0e. To fix this issue, it is recommended to deploy a patch.	4.3	More Deta
CVE-2026-119414	Bitwarden Server before 2026.10.1 on Entity Framework backends contains an authorization bypass vulnerability that allows organization members to add ciphers to collections they cannot edit. Attackers can call POST /api/ciphers/create, where a nulled UserId is treated as administrative, to inject vault items synced to read-only or inaccessible collections' members.	4.3	More Deta
CVE-2026-118578	A security flaw has been discovered in maotoumao MusicFreeDesktop 0.0.6/0.0.7/0.0.8. The affected element is an unknown function of the component Request Forwarder. The manipulation results in information disclosure. The attack can only be performed from the local network. The exploit has been released to the public and may be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	4.3	More Deta
CVE-2026-88078	Improper verification of cryptographic signature in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	4.3	More Deta
CVE-2026-104308	IBM Langflow OSS 1.0.0 through 1.12.3 could allow a remote authenticated attacker to cause a denial of service due to improper neutralization of special elements used in an OS command.	4.3	More Deta
CVE-2026-119664	Tamery (formerly Conar) 0.26.1 before 0.99.0 contains an authorization bypass vulnerability in the cloud sync API chatsMessages.update handler, which leaves the client-supplied chatId writable. Authenticated Pro subscribers who know another user's chat ID can move messages with arbitrary parts and metadata into the victim's AI chat history.	4.3	More Deta
CVE-2026-116610	The Clean Login plugin for WordPress is vulnerable to Missing Authorization in versions up to, and including, 1.20.1 due to a missing capability check on the CleanLogin_Shortcode::get_pages_with_shortcodes() function hooked to the save_post action. This makes it possible for authenticated attackers, with Contributor-level access and above, to overwrite the plugin's cl_login_url/cl_login_id/cl_register_url/cl_register_id/cl_restore_url/cl_restore_id/cl_edit_url/cl_edit_id/cl_change_password_url/cl_change_password_id options with the ID and permalink of a post they themselves authored — simply by embedding the plugin's shortcodes in their own post content.	4.3	More Deta
CVE-2026-104310	IBM Langflow OSS 1.0.0 through 1.12.3 could allow a remote authenticated attacker to obtain sensitive information due to a server-side request forgery (SSRF) vulnerability.	4.3	More Deta
CVE-2026-115962	Authentication Bypass by Spoofing vulnerability in myCred myCred mycred allows Identity Spoofing.This issue affects myCred: from n/a through 4.0.1.	4.3	More Deta
CVE-	Collabora Online is a collaborative online office suite based on LibreOffice technology. Prior to 24.04.18 and 25.04.11, several document operations delegated to `LibreOfficeKit` in the per-document kit process fail to enforce a session's read-only state. A read-only user, such as a		

2026-46499	viewer-role WOPI user, can send crafted `WebSocket` messages to execute document-mutating `UNO` commands and dialog operations despite the read-only interface. The changes can mislead co-viewers within the live session, or an authorized editor sharing the session can unknowingly save the modifications. The read-only attacker cannot save the document directly, and changes are discarded when the kit session ends unless an authorized editor saves them. This issue is fixed in versions 24.04.18 and 25.04.11.	4.3	More Deta
CVE-2026-109979	The Related Posts for WordPress plugin for WordPress is vulnerable to Sensitive Information Exposure in versions up to, and including, 3.0.0 via the 'rp4wp_create_link' parameter of the hidden 'rp4wp_link_related' admin page. The handle_create_link() handler verifies the nonce and that the current user can edit the parent post, but never checks that the attacker-supplied child post ID is one the user is allowed to read; LinkRepository::insert() stores the arbitrary child ID without validation, and ManageLinks::render() later calls LinkRepository::get_children() in its no-extra-args fast path, which falls through to array_map('get_post', $child_ids) — bypassing read_private_posts/read_post capability checks — and then echoes esc_html($child->post_title) in the parent's editor meta box. This makes it possible for authenticated attackers, with Contributor-level access and above, to read the titles of arbitrary non-public posts (drafts, pending, private, future, trashed) authored by higher-privileged users by linking those post IDs to a draft they own and then reading the resulting meta box.	4.3	More Deta
CVE-2026-117605	nopCommerce before 5.00.0 contains a missing authorization vulnerability in the admin ProductController RelatedProductAddPopup, CrossSellProductAddPopup and AssociatedProductAddPopup handlers that fail to verify parent product ownership. Authenticated vendors can submit another vendor's product id as model.ProductId to inject their products into the victim's related-products, cross-sell and grouped-product listings.	4.3	More Deta
CVE-2026-93009	A flaw was found in dnsmasq. The DHCPv6 client hostname parser can read one byte past the end of a crafted FQDN option because it checks the next label length before confirming the pointer is still inside the option. An attacker on the local network can trigger this with a single DHCPv6 packet. The extra byte is not returned to the client or logged, and no crash has been demonstrated.	4.3	More Deta
CVE-2026-93010	A flaw was found in dnsmasq. When DHCP leasequery is enabled without listing allowed source addresses, the server does not check who sent the query. A host on the local network can request DHCP lease records and learn assigned addresses, MAC addresses, hostnames, and related lease metadata. The feature is off unless an administrator turns it on.	4.3	More Deta
CVE-2026-103393	An Out-of-Bounds Read vulnerability in the VRRP implementation in Juniper Networks Session Smart Router allows an L2-adjacent attacker to read stale memory contents or cause a system fault via a specially crafted VRRPv3 advertisement.	4.3	More Deta
CVE-2026-62019	Missing Authorization vulnerability in Liquid Web / StellarWP BookIt bookit allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects BookIt: from n/a through 2.6.0.6.	4.3	More Deta
CVE-2026-62023	Missing Authorization vulnerability in Unlimited Elements Unlimited Elements For Elementor (Free Widgets, Addons, Templates) unlimited-elements-for-elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Unlimited Elements For Elementor (Free Widgets, Addons, Templates): from n/a through 2.0.26.	4.3	More Deta
CVE-2026-62047	Missing Authorization vulnerability in Liquid Web / StellarWP Event Tickets event-tickets allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Event Tickets: from n/a through 5.30.2.	4.3	More Deta
CVE-2026-119542	A flaw was found in the Ickle query parser in Infinispan. A query containing deeply nested predicates can cause recursive parsing to exhaust the Java thread stack and throw an uncaught StackOverflowError. An authenticated user with BULK_READ permission who can submit a cache query may trigger the issue, potentially affecting availability.	4.3	More Deta
CVE-2026-115605	Missing Authorization vulnerability in Brainstorm Force SureDash suredash allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects SureDash: from n/a through 1.12.3.	4.3	More Deta
CVE-2026-55146	LORIS (Longitudinal Online Research and Imaging System) is a self-hosted web application that provides data- and project-management for neuroimaging research. In versions from 16.0.0 prior to 27.0.4 and from 28.0.0 prior to 28.0.2, the `issue_tracker` backend does not correctly verify edit access permissions, although the frontend restricts which issues a user may edit. An authenticated user can submit backend changes to issues outside the user's permitted edit scope. Deployments that no longer use Issue Tracker can disable the module to remove access to the endpoint. This issue is fixed in versions 27.0.4 and 28.0.2.	4.3	More Deta
CVE-2026-118271	A security vulnerability has been detected in a2ui-project a2ui up to 0.10.6. This impacts an unknown function of the file renderers/web_core/src/v0_9/rendering/data-context.ts of the component data-context Resolver. Such manipulation leads to resource consumption. The attack may be performed from remote. The exploit has been disclosed publicly and may be used. The name of the patch is eb314e14fabd29cfb4a74e1202afc4fe2081efa2. Applying a patch is advised to resolve this issue.	4.3	More Deta
CVE-2026-118272	A vulnerability was detected in a2ui-project a2ui up to 0.10.6. Affected is the function DataContext.dispatchExpressionError of the file renderers/web_core/src/v0_9/rendering/data-context.ts of the component Error Handler. Performing a manipulation results in information exposure through error message. It is possible to initiate the attack remotely. The exploit is now public and may be used. The patch is named 8f149a1c7b0ce1fa8e93ac3adfa5fda960faeb01. It is suggested to install a patch to address this issue.	4.3	More Deta
CVE-2026-86386	Dell PowerProtect Data Domain Management Center, Feature Release versions 7.7.1.0 through 8.8, LTS2024 release versions 7.13.1.0 through 7.13.1.80, LTS2025 release versions 8.3.1.0 through 8.3.1.40, LTS2026 release versions 8.6.1.0 through 8.6.1.20, contain an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Information disclosure.	4.3	More Deta
CVE-2026-119730	Maxthon Browser for Android before 7.5.8.103 contains an address bar spoofing vulnerability that allows remote attackers to misrepresent a page's origin by exploiting the lack of a persistent fullscreen notification or trusted origin indicator when the Fullscreen API is invoked. Attackers can craft a malicious web page that renders a counterfeit address bar showing a trusted domain while displaying attacker-controlled content, tricking users who perform a single tap to enter fullscreen into disclosing credentials via phishing.	4.3	More Deta
CVE-2026-115712	Incorrect Authorization (CWE-863) in Elastic Cloud Enterprise (ECE) can lead to unauthorized modification of platform-level settings via Accessing Functionality Not Properly Constrained by ACLs (CAPEC-1). An authenticated user with read-only access to the platform can change an installation-wide account setting that only platform administrators are permitted to change.	4.3	More Deta
CVE-2026-25448	Missing Authorization vulnerability in weDevs WP ERP erp allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP ERP: from n/a through 1.17.10.	4.3	More Deta
CVE-2026-119715	NocoDB before 2026.08.0 contains a clickjacking vulnerability that allows any origin to frame the authenticated interface because no X-Frame-Options or CSP frame-ancestors headers are sent. Attackers can overlay a signed-in user's session from a malicious page, tricking clicks that modify or delete records, change sharing settings, or invite collaborators.	4.3	More Deta

CVE-2026-85655	The Enable Media Replace plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 4.2.2. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with author-level access and above, to modify the post_content of any published post referencing the replaced media — including Administrator-owned posts — making changes immediately visible to unauthenticated visitors. The doReplaceQuery() method performs a database-wide search-and-replace across all posts containing the old media URL without any per-post capability check, meaning a single Author-triggered request can silently overwrite a large number of posts that WordPress's standard admin UI and REST API would otherwise forbid that user from editing.	4.3	More Deta
CVE-2026-116406	Missing Authorization vulnerability in Webba Plugins Webba Booking webba-booking-lite allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Webba Booking: from n/a through 6.5.4.	4.3	More Deta
CVE-2026-22386	Missing Authorization vulnerability in Ahmad WP Job Portal wp-job-portal allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Job Portal: from n/a through 2.7.1.	4.3	More Deta
CVE-2026-109980	The Related Posts for WordPress plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.0.0 via the 'rp4wp_view' parameter. This makes it possible for authenticated attackers, with contributor-level access and above, to extract the titles and publication dates of all private posts site-wide, normally restricted to Editor-level users and above. The page's existing authorization check only verifies edit_posts and edit_post on a parent post the attacker owns, both of which any Contributor satisfies, leaving no effective gate against reading other authors' private posts.	4.3	More Deta
CVE-2026-119576	ArcadeDB from 21.12.1 before 26.10.2 contains an authorization bypass vulnerability that allows users with only readRecord to replace the shared GraphQL schema via the read-only query endpoint. Attackers can send a GraphQL type definition with a crafted @sql directive to /api/v1/query/{database}, altering query results returned to other users including administrators.	4.3	More Deta
CVE-2026-119329	Immich is a high-performance self-hosted photo and video management solution. Prior to 3.0.0, GET /api/map/markers used server/src/services/map.service.ts to add partner owner identifiers when withPartners=true, while server/src/repositories/map.repository.ts applied Archive visibility to every selected owner when isArchived=true. A view-only partner could therefore enumerate the GPS coordinates and existence of a sharer's archived photos or videos even though the timeline and direct-access paths exclude archived partner assets. The exposure is limited to location metadata and asset identifiers because image bytes remain protected by checkPartnerAccess. This issue is fixed in version 3.0.0.	4.3	More Deta
CVE-2026-119596	UNIT3D through 9.2.0 contains a missing authorization vulnerability in PlaylistZipController::show that allows authenticated users to download other members' private playlists. Attackers can enumerate sequential playlist ids at the /playlist-zips/{playlist} endpoint to obtain zips of all torrents, disclosing private collection membership.	4.3	More Deta
CVE-2026-118092	Missing Authorization vulnerability in StylemixThemes MasterStudy LMS masterstudy-lms-learning-management-system allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects MasterStudy LMS: from n/a through 3.7.55.	4.3	More Deta
CVE-2026-119598	Miaomiaowu before 0.9.3 contains an insecure direct object reference vulnerability in /api/user/proxy-provider-configs that allows authenticated users to read other users' configurations. Attackers can iterate the global auto-increment external_subscription_id parameter to disclose override scripts, filter rules, custom request headers and health-check URLs.	4.3	More Deta
CVE-2026-118947	A flaw was found in the UMA resource registration endpoint of the keycloak-services component, which provides the core logic for Keycloak's authorization and identity services. The issue occurs when remote resource management is enabled, allowing an authenticated user with specific permissions to update resources they do not own by providing a target resource ID in a request. This can lead to unauthorized modification of resource configurations, such as names, URIs, and scopes.	4.3	More Deta
CVE-2026-119599	AxonHub through 1.0.0-beta11 contains a privilege escalation vulnerability that allows project users to assign system-level scopes by creating service_account API keys with unvalidated scopes. Attackers holding write_api_keys can mint keys with read_channels and query /admin/graphql to read every channel's configuration, including base URLs and model lists.	4.3	More Deta
CVE-2026-119658	PowerDNS-Admin through 2026.08.1 contains an authorization bypass vulnerability that allows authenticated User-role accounts to refresh secondary zones they cannot access by supplying a different 'domain' field in the JSON body. Attackers authorized for any one zone can force axfr-retrieve transfers of other users' secondary zones and infer zone existence from differing responses.	4.3	More Deta
CVE-2026-119663	Tamery (formerly Conar) 0.32.0 before 0.99.0 contains a broken authorization vulnerability in the cloud sync API connectionsResources.create handler that allows authenticated users to attach resources to other users' connections. Attackers owning one connection can include a victim's connectionId in a batch request to insert attacker-named resource rows listed by the victim's client.	4.3	More Deta
CVE-2026-110983	The WP Photo Album Plus WordPress plugin before 9.3.04.004 does not verify the origin or a security token for one of its comment-management requests, allowing attackers to delete photo comments by tricking a logged-in user who holds comment-moderation rights into loading a crafted page.	4.3	More Deta
CVE-2026-107268	Insertion of Sensitive Information Into Sent Data vulnerability in Drupal Two Factor Authentication - TFA / Passwordless Login allows Forceful Browsing. This issue affects Two Factor Authentication - TFA / Passwordless Login versions: from 0.0.0 to 5.4.1, from 5.5.0 to 5.5.2.	4.3	More Deta
CVE-2026-110183	PostgreSQL Anonymizer contains a vulnerability related to static masking and statistics persistence. Statistics pertaining to the original data remain visible in pg_stats until an ANALYZE operation is performed on the table, either manually or by autovacuum. This issue is fixed in PostgreSQL Anonymizer 3.3.0 and later versions.	4.3	More Deta
CVE-2026-108763	The Wallet System for WooCommerce WordPress plugin before 2.8.2 does not restrict its KYC document submission handler to the current user's own account, taking the target user ID from a client-supplied request field with no ownership or capability check, allowing authenticated users with minimal privileges such as Subscriber or Customer to overwrite the KYC documents and verification status of any other user, including an administrator.	4.3	More Deta
CVE-2026-110182	PostgreSQL Anonymizer contains a vulnerability related to the anon.partial() and anon.partial_email() functions. These function can reveal the while data if the data is small enough. The issue is fixed in PostgreSQL Anonymizer 3.3.0 and later versions.	4.3	More Deta
CVE-2026-20942	Improper restriction of rendered ui layers or frames in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	4.3	More Deta
	The Content Egg – Affiliate Product Importer & Price Comparison plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 12.0.0 This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for		

CVE-2026-119087	authenticated attackers, with author-level access and above, to create posts attributed to another user's account — typically an administrator — by supplying an admin-owned preset_id, causing wp_insert_post to record the administrator as post_author. This includes the ability to create published posts when the attacker already holds publish_posts capability for the preset's post type, resulting in administrator-attributed published content created by a lower-privileged user.	4.3	More Deta
CVE-2026-107312	Allocation of Resources Without Limits or Throttling vulnerability in Drupal Examples for Developers allows Excessive Allocation. This issue affects Examples for Developers versions: from 0.0.0 to 4.0.7.	4.3	More Deta
CVE-2026-107310	Server-Side Request Forgery (SSRF) vulnerability in Drupal Freelinking allows Server Side Request Forgery. This issue affects Freelinking versions: from 0.0.0 to 4.0.3.	4.3	More Deta
CVE-2026-107307	Incorrect Authorization vulnerability in Drupal SmartLinker AI allows Forceful Browsing. This issue affects SmartLinker AI versions: from 0.0.0 to 1.0.3.	4.3	More Deta
CVE-2026-119652	HuLa-Server through 3.0.7 contains an insecure direct object reference vulnerability in FriendController.friendList that allows authenticated users to view other users' friend lists by supplying a uid parameter. Attackers can send GET requests to /user/friend/page with a victim's uid, bypassing the missing administrator or owner check to read any user's contact list.	4.3	More Deta
CVE-2026-109592	The OpenStation: Desktop Windows, Dock & Virtual Desktops for WP Admin plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.1.16. 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 modify arbitrary other users' placement rows (position, sort order, parent folder, and meta) and read serialized metadata — including title, permalink, and post status — of the entities those orphaned placements reference. Exploitation requires at least one orphaned placement to exist — a state produced naturally by the plugin's own trash cascade, which marks a parent folder as trashed while leaving child placements' parent_id intact — and the attacker must first self-enable OpenStation via the save-openstation AJAX endpoint, which requires only the 'read' capability held by every default WordPress role. This was also independently found by the OpenStation team.	4.3	More Deta
CVE-2026-119059	The Content Egg plugin for WordPress is vulnerable to unauthorized modification of data due to a missing per-post capability check on the ajaxUpdateProducts() function in versions up to, and including, 12.0.0. The handler verifies a static nonce ('contentegg_metabox') and the generic 'edit_posts' capability, but trusts the attacker-supplied $_POST['post_id'] verbatim and never calls current_user_can('edit_post', $post_id) — the per-object check that its sibling save_post handler saveMeta() correctly performs. This makes it possible for authenticated attackers, with contributor-level access and above, to modify Content Egg product data (_cegg_data_*) and update-timestamp post meta on arbitrary posts, including those owned by administrators.	4.3	More Deta
CVE-2026-50543	Xibo is an open source digital signage platform with a web content management system and Windows display player software. Prior to 4.4.3, missing authorization on `POST /displaygroup/criteria/{displayGroupId}` allows an authenticated user to send criteria updates to any display via `XMR`. These criteria determine schedule changes and can alter playback, for example by causing content scheduled for rainy weather to play when it is not raining. Exploitation requires `Schedule Criteria` to be in use on the CMS. This issue is fixed in version 4.4.3.	4.3	More Deta
CVE-2026-119547	Forgejo through 15.0.11, 16.0.0 through 16.0.7, and 17.0.0 through 17.0.1 contains an information disclosure vulnerability in the GetPublicKey API handler that lacks an ownership check on key lookups. Authenticated users with a read:user token or session can enumerate sequential key IDs to obtain titles, fingerprints and public key material of other users' SSH, deploy and principal keys.	4.3	More Deta
CVE-2026-119121	Crawl4AI from 0.9.0 before 0.9.5 contains a JavaScript injection vulnerability in the Docker API server that allows authenticated API clients to run arbitrary JavaScript in the crawl page via allowlisted css_selector and wait_for fields. Attackers can inject quotes into css_selector or supply js: conditions in wait_for, bypassing the js_code block to alter page state and returned crawl content.	4.3	More Deta
CVE-2026-112374	FOSSBilling before 0.8.9 contains a Cross-Site Request Forgery vulnerability in the staff guest login endpoint (POST /api/guest/staff/login) that allows remote attackers to force authentication because checkGuestClientAuthentication() only allowlists client_login and client_create, leaving staff_login without CSRF or Origin validation. Attackers can host an auto-submitting HTML form with attacker-controlled credentials to silently log a victim's browser into the attacker's staff account.	4.3	More Deta
CVE-2026-111502	Dell OpenManage Enterprise, versions prior to 4.8.0, contains an Insufficiently Protected Credentials vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Information disclosure.	4.3	More Deta
CVE-2026-115300	The Contact Form by Supsystic WordPress plugin before 1.11.1 does not validate a CSRF token or request origin on two administrator-only actions that bulk-delete captured form submissions and wipe a form's statistics, allowing attackers to permanently destroy a site's stored contact leads and analytics by tricking a logged-in administrator into sending a forged request.	4.3	More Deta
CVE-2026-119429	phpMyAdmin through 5.2.3 contains a missing re-authentication vulnerability that allows authenticated attackers to remove two-factor authentication by posting the 2fa key to /config/set. Attackers holding a hijacked session can submit key=2fa with a null JSON value to SetConfigController, stripping 2FA so later logins require only the MySQL password.	4.3	More Deta
CVE-2026-85330	Incorrect authorization in Microsoft Edge for Android allows an unauthorized attacker to bypass a security feature over a network.	4.3	More Deta
CVE-2026-119648	Tencent BlueKing CMDB (bk-cmdb) through 3.14.6 contains a missing authorization vulnerability that allows authenticated users to view hosts of other businesses via POST /api/v3/hosts/search/asstdetail. Attackers can submit host search conditions targeting other businesses or omitting business filters to retrieve host attributes and topology association details, because the route is mapped to SkipAction and SearchHostWithAsstDetail skips AuthorizeSearchHost.	4.3	More Deta
CVE-2026-119556	Moodle 4.2.0 through 4.5.15, 5.0.0 through 5.0.11, 5.1.0 through 5.1.8, 5.2.0 through 5.2.4, and 5.3.0 contain a missing capability check in the core_grades_get_gradeitems web service that allows enrolled students to view hidden grade items. Authenticated course users can call the AJAX or mobile web service to list hidden grade item ids, names, and categories that the gradebook conceals from them.	4.3	More Deta
CVE-2026-119565	Plausible Analytics through 3.2.1 contains a mass assignment vulnerability in update_traffic_change_notification that allows authenticated site editors to reassign notifications by supplying a site_id parameter. Attackers can submit traffic_change_notification[site_id] set to another site's primary key via PUT /sites/:domain/traffic-change-notification/:type to receive that site's traffic alerts and visitor figures.	4.3	More Deta
CVE-2026-104674	Missing Authorization vulnerability in Arraytics Booktics booktics allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Booktics: from n/a through 1.0.31.	4.3	More Deta

CVE-2026-119653	Nging through 5.3.5 contains an information disclosure vulnerability that allows any authenticated backend user to list host directories by abusing the public-tagged /user/autocomplete_path endpoint. Low-privileged users without file-manager permission can supply arbitrary paths in the query parameter to enumerate directories readable by the Nging process and confirm specific files exist.	4.3	More Deta
CVE-2026-119647	RuoYi-Vue-Plus through 6.0.0 contains an authorization bypass vulnerability in SysUserServiceImpl.selectUserListByDept that allows authenticated users to read users of other departments. Users holding system:user:list under a department-restricted role can request GET /system/user/list/dept/{deptId} with any department id to obtain usernames, nicknames, account status, last login IP and time, and remarks.	4.3	More Deta
CVE-2026-119555	Moodle 4.2.0 through 4.5.15, 5.0.0 through 5.0.11, 5.1.0 through 5.1.8, 5.2.0 through 5.2.4, and 5.3.0 contain an information disclosure vulnerability in the core_grades_get_feedback web service. The service lacks group-membership and enrolment checks, so non-editing teachers can iterate userid values to read other groups' grade feedback and users' names and identity fields such as email.	4.3	More Deta
CVE-2026-119646	Open Web Analytics before 1.14.1 contains an authorization vulnerability that allows authenticated users to read other sites' report data because clickstream and transaction reports are not scoped to the authorized siteId. Users with view_reports on one site can supply that siteId with another site's session_id or order_id to read its visit history, IP addresses, user agents and order data.	4.3	More Deta
CVE-2026-42694	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Themeum Kirki kirki allows Code Injection.This issue affects Kirki: from n/a through 6.4.0.	4.3	More Deta
CVE-2026-67077	HCL BigFix AEX is affected by a Server-Side Request Forgery vulnerability, which could allow an attacker to cause the application to send unauthorized requests to external resources. Successful exploitation could lead to access to unintended services, sensitive information disclosure, or unauthorized actions through the affected application.	4.2	More Deta
CVE-2026-119298	croc is a tool that allows any two computers to simply and securely transfer files and folders. Prior to 11.5.2, the receive-side file-readiness loop in src/croc/croc.go treats any sender-controlled basename beginning with croc-stdin- as a trusted text-transfer artifact even when SendingText is false. This skips askReceiveOverwrite and rename handling for a predictable exact-name collision in the receiver's working directory, allowing a remote sender whose transfer the user accepts to overwrite or truncate a matching regular file through recipientInitializeFile, or to remove and replace a matching destination with an empty file or an in-directory symlink through createEmptyFileAndFinish, without confirmation. The impact is limited to pre-existing names in the croc-stdin- namespace that the sender can predict; other filenames retain the prompt, dotfiles outside that namespace are not reachable, and symlink targets remain confined to the receive directory. This issue is fixed in version 11.5.2.	4.2	More Deta
CVE-2026-119048	JeeSite 5.11.0 through 5.19.1 contains an insecure direct object reference vulnerability in the AI CMS chat module that allows authenticated users to access other users' conversations due to missing and reversed ownership checks. Attackers who know or derive a victim's conversation id can call /a/cms/chat/message, /a/cms/chat/delete, or /a/cms/chat/completions to read, delete, or append to the victim's AI chat transcripts.	4.2	More Deta
CVE-2026-119562	phpMyAdmin through 5.2.3 contains an sql injection vulnerability that allows authenticated users to inject SQL by supplying unescaped col_extra and col_attribute values to /database/central-columns. Attackers can inject SQL into pma__central_columns INSERT and UPDATE queries run with controluser privileges, reading or modifying other users' configuration-storage data.	4.2	More Deta
CVE-2026-118030	A flaw was found in the HOTP authentication mechanism of the keycloak-services component, which provides identity and access management services. The issue occurs because the system validates a one-time password and updates its internal counter in two separate steps without proper locking. An attacker with a users password could exploit this timing gap to use a single one-time code to log in multiple times simultaneously.	4.2	More Deta
CVE-2026-119661	ShowDoc through 3.9.5 contains an authorization bypass vulnerability in the api/paramDescLib/deleteEntries endpoint that checks edit permission only for the first supplied entry id. Authenticated attackers can place their own entry id first and append other users' entry ids to permanently delete those parameter-description entries.	4.2	More Deta
CVE-2026-107261	Authentication Bypass Using an Alternate Path or Channel vulnerability in Drupal Authenticator Login Plus (2FA) allows Authentication Bypass. This issue affects Authenticator Login Plus (2FA) versions: from 0.0.0 to 1.0.1.	4.2	More Deta
CVE-2026-107745	The AI Engine – The Chatbot, AI Framework & MCP for WordPress plugin for WordPress is vulnerable to limited media file deletion due to insufficient file path validation in the upload_file function in all versions up to, and including, 3.8.4 This makes it possible for authenticated attackers, with subscriber-level access and above, to delete arbitrary media files on the server. This requires the administrator to have enabled the Public API option, and exploitation depends on the hourly cleanup_files task running after the malicious upload.	4.2	More Deta
CVE-2026-116251	pgAdmin 4 did not invalidate a user's existing sessions when their password changed, either through the user's own change password dialog or through an administrator resetting it in User Management. A session established before the change, for example on another device or by someone who had obtained the old password or a session cookie, therefore stayed logged in after the change, which is the step a user or administrator takes precisely to cut such access off. It remained usable until it expired. The fix rotates the user's session identifier (fs_uniquifier) whenever the password is changed, so every other session of that user is logged out. The session that made the change is logged in again and keeps its database connections. Saved server passwords, including those for shared servers, are re-encrypted under the new key; any that cannot be decrypted are cleared and the user is told. If re-encryption fails, the sessions are still revoked and the saved passwords are cleared rather than the change failing. This issue affects pgAdmin 4: before 9.19.	4.2	More Deta
CVE-2026-119427	phpMyAdmin through 5.2.3 contains an sql injection vulnerability in Designer saveSetting() that allows authenticated users to inject SQL via unescaped json_encode() output. Attackers can send crafted index or value parameters with operation=save_setting_value to /database/designer to overwrite other users' designer settings or run controluser subqueries.	4.2	More Deta
CVE-2026-81472	Dell iDRAC Service Module (iSM) for Windows, Dell iDRAC Service Module (iSM) for Linux, and Dell iDRAC Service Module (iSM) for ESXi, versions prior to 6.1.1.0, contains an Improper Control of Generation of Code ('Code Injection') vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges.	4.2	More Deta
CVE-2026-115224	The Customer Engagement System WordPress plugin before 2.0.2 does not safely build the SQL statements that store a popup's page and category visibility rules, concatenating request-supplied ID values directly into an INSERT statement with no parameter binding or integer cast, allowing an authenticated administrator to inject arbitrary SQL and read the contents of the WordPress database.	4.1	More Deta
CVE-2026-117572	The WP Visitor Statistics (Real Time Traffic) WordPress plugin before 8.8 does not sanitize and escape a parameter before using it in a SQL statement, allowing high-privilege users such as administrators to perform SQL injection attacks.	4.1	More Deta
CVE-2026-85007	The Video Player for YouTube WordPress plugin before 2.1.4 does not perform a capability check on its player-preset AJAX handler, allowing users with the Contributor role and above to read the site-wide player-preset configuration, and in versions before 2.1.1 to modify and delete it as well.	3.8	More Deta
CVE-	The Royal MCP WordPress plugin before 1.5.10 does not perform an object-level permission check before duplicating a requested page, relying on		

2026-111961	a generic capability, which allows users with contributor-level access to read the full content of any private or draft page and to publish it without holding the publish capability.	3.8	More Deta
CVE-2026-107306	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Menu Link Attributes allows Stored XSS. This issue affects Menu Link Attributes versions: from 0.0.0 to 1.8.0.	3.8	More Deta
CVE-2026-106647	The Royal Addons for Elementor WordPress plugin before 1.7.1070 does not scope a contact form's email delivery configuration to the form's own document or owner, instead storing it in a site-global namespace keyed only on a non-secret, author-chosen identifier that is exposed in public page source, allowing users with the Author role or above to overwrite another user's form configuration and have that form's submissions delivered to an attacker-controlled address.	3.8	More Deta
CVE-2026-111032	The Welcart e-Commerce WordPress plugin before 2.12.6 does not properly verify authorization against the targeted product before processing SKU changes, because its capability check is not tied to the product being edited, allowing any authenticated user with Author-level access or higher to read, modify, create, delete and re-order the SKU data (including prices, confidential cost prices and stock levels) of any product, including those belonging to other users.	3.8	More Deta
CVE-2026-118371	LibreSSL through 4.4.0 contains a CRLF injection vulnerability in the libcrypto OCSP_sendreq_new() and OCSP_parse_url() functions, which write unvalidated request paths into the OCSP POST request line. Attackers can embed carriage return and line feed characters in a certificate's Authority Information Access OCSP URI to inject HTTP headers or split requests sent to responders and proxies.	3.7	More Deta
CVE-2026-119417	CakePHP 4.5.12, 4.6.5, 5.1.8 through 5.1.10, 5.2.14 through 5.2.15, 5.3.7, and 5.4.0 through 5.4.3 contain an email header injection vulnerability because SmtpTransport and MailTransport strip only CRLF pairs from header values, an incomplete fix for CVE-2026-77634. Attackers controlling custom headers set via Message::setHeaders() or Message::addHeaders() can insert a bare CR or LF to inject headers like Bcc, redirecting or altering outgoing mail.	3.7	More Deta
CVE-2026-55612	uhttpd is a small HTTP server. In unpatched repository snapshots, `client_poll_post_data()` in `client.c` consumes an invalid chunk-length line, such as a size exceeding INT_MAX, then clears `r->content_length` and `r->transfer_chunked` without draining the remaining body or setting `request.connection_close`. The completion check treats the chunked POST as finished and the keep-alive parser returns to `CLIENT_STATE_INIT`. Attacker-controlled body bytes aligned as a complete HTTP request are then parsed and processed as another request on the same connection, causing HTTP request smuggling and request-boundary desynchronization. Commits b78f518478794e16ba3568fc1258e40bf3e8eb3b and 34460b8211d676ef1b9f40d6b775c5e112933690 patch the issue.	3.7	More Deta
CVE-2026-119415	CakePHP through 5.4.3 contains a header injection vulnerability in FormDataPart that allows attackers to inject MIME part headers via unsanitized Content-Type and Content-ID values. Attackers can supply CR/LF sequences in attachment MIME types or Content-IDs passed to Message::setAttachments() or HTTP client multipart data to add arbitrary headers or content.	3.7	More Deta
CVE-2026-21830	HCL BigFix AEX product is affected by a vulnerability in the aws-sdk package.. It may cause AWS API requests to be sent to unintended or non-AWS endpoints.	3.7	More Deta
CVE-2026-118258	i18next-http-backend is a backend layer for i18next that loads translation resources in Node.js, browsers, and Deno. Prior to 4.0.4, interpolateUrl inserts unencoded language and namespace values into loadPath or addPath templates without rejecting ampersand (&), equals (=), or semicolon (;) query separators. When a template places lng or ns in the query string and an attacker controls that value, the attacker can add or override parameters on browser or server-side translation requests, potentially exposing other namespaces or tenants or changing backend behavior through the application's network position and credentials. This vulnerability is the result of an incomplete fix for CVE-2026-41691. This issue is fixed in version 4.0.4.	3.7	More Deta
CVE-2026-118373	LibreSSL ocspcheck through 4.4.0 contains a cleartext transmission vulnerability because url2host() discards the OCSP URL scheme and http_alloc() only selects TLS for port 443. On-path network attackers can read OCSP requests sent to https responder URLs on non-443 ports, exposing certificate serial numbers, issuer hashes, and nonces.	3.7	More Deta
CVE-2026-115303	The Contact Form by Supsystic WordPress plugin before 1.11.1 does not strip CR/LF characters or re-validate submitted field values before concatenating them into outgoing email headers when a form is configured to map a submitted field into its Reply-To, From or Cc header, allowing unauthenticated users to inject arbitrary email headers such as additional Bcc or Cc recipients into the notification email.	3.7	More Deta
CVE-2026-61694	go-xrpl is a Go implementation of the XRP Ledger protocol. In versions through the June 18, 2026 revision identified by the advisory, `ParseMPTAmountBinary` in `internal/ledger/state/ripple_state.go` converts the eight-byte MPT magnitude using `num.Int64()` without checking that it fits in 63 bits. A positive magnitude of at least 2^63 silently wraps into a negative amount without an error. `ParseEscrow` passes 33-byte `sfAmount` fields to the parser and stores `MPTRaw()` in `EscrowData.MPTAmount`, causing incorrect downstream calculations and divergence from rippled's interpretation of the same escrow entry. Independently, `readMPTAmount` in `internal/tx/ledgerfields/decode_stream.go` accepts over-limit magnitudes and surfaces large decimal strings without enforcing the maximum signed 64-bit value. The public codec in codec/binarycodec/types/amount.go already rejects these values, leaving the internal decoders inconsistent with that safe path. A source fix is available in commit 9dbd3935ed6c54f0232f2291edf9c012a0900dd5.	3.7	More Deta
CVE-2026-118780	Forge (also called node-forge) is a native implementation of Transport Layer Security in JavaScript. Prior to 1.4.1, the affected implementation used pki.verifyCertificateChain(), pki.createCaStore(), duplicate subject names to process the relevant input or security decision. node-forge modified the CA store while trying certificates that shared a subject name during pki.verifyCertificateChain(). A failed chain verification could permanently remove trusted CA certificates from the store, causing later valid chains to fail and creating a persistent availability impact for applications that reused the store. This issue is fixed in version 1.4.1.	3.7	More Deta
CVE-2026-119280	MariaDB Connector/J is used to connect applications developed in Java to MariaDB and MySQL databases. From 3.0.0 until 3.3.7, 3.4.5, and 3.5.11, the MariaDbPoolConnection.recover() and MariaDbPoolPinnedConnection.recover() implementations trusted the gtrid_length and bqual_length columns returned by XA RECOVER. The methods allocated and split Xid byte arrays without validating the lengths against Xid.MAXGTRIDSIZE, Xid.MAXBQUALSIZE, or the actual data payload. A malicious or compromised server, or a machine-in-the-middle attacker, could cause large allocations, NegativeArraySizeException, or ArrayIndexOutOfBoundsException during XA recovery. This issue is fixed in versions 3.3.7, 3.4.5, and 3.5.11.	3.7	More Deta
CVE-2026-119571	Parse Server from 9.7.0 before 9.10.5-alpha.10 contains an authorization flaw that applies _Installation updates addressed by object ID to the installation named in the X-Parse-Installation-Id header. When protectedFieldsTriggerExempt is enabled, attackers knowing another installation's object ID can make a beforeSave trigger process that installation's protected fields while writing elsewhere.	3.7	More Deta
CVE-2026-118681	go-chi chi before 5.5.0 contains an authentication bypass in middleware.SupressNotFound, which calls Match with the live routing context and leaves a mounted router's parameter and child suffix in place for dispatch against the outer router. Unauthenticated attackers can request a mounted path whose suffix matches an outer public route, skipping the mounted authentication middleware and retrieving tenant-scoped data when that outer handler trusts the retained mount parameter.	3.7	More Deta

CVE-2026-103394	An Improper Initialization vulnerability in the SSR software in Juniper Networks Session Smart Router allows an attacker to decrypt traffic or cause a denial of service via security policy assignment.	3.7	More Deta
CVE-2026-119428	phpMyAdmin through 5.2.3 contains a server-side request forgery vulnerability that allows unauthenticated attackers to trigger outbound connections via setup/validate.php, which lacks the setup-disabled guard. Attackers can POST attacker-chosen host and port values reaching Validator::testDBConnection() to open MySQL-protocol connections and probe internal ports using returned error messages.	3.7	More Deta
CVE-2026-119123	ImageMagick before 7.1.2-34 contains a stack overflow vulnerability in the TIFF decoder that occurs when the DNG decoder is disabled. Attackers can supply a crafted image file for processing to trigger the stack overflow and crash the application, causing denial of service.	3.7	More Deta
CVE-2026-118691	xianyu-auto-reply-fix through 2.0.7 contains a missing authorization vulnerability in the POST /send-message endpoint that allows unauthenticated attackers to send messages from other users' accounts using publicly known default API secrets. Attackers can supply the hard-coded api_key and another user's cookie_id, plus chosen chat_id, to_user_id and message values, to send arbitrary Xianyu messages to buyers from that merchant account.	3.7	More Deta
CVE-2026-119602	libmspack through 0.11alpha contains an uninitialized memory disclosure vulnerability in the MS-ZIP decompressor that allows attackers to leak heap data via unchecked back-reference distances. Attackers can supply a crafted MS-ZIP CAB file whose first block begins with a back-reference, causing cabd->extract() to write up to 32 KiB of stale heap memory into extracted output.	3.7	More Deta
CVE-2026-107309	Missing Authorization vulnerability in Drupal Easy Breadcrumb allows Forceful Browsing. This issue affects Easy Breadcrumb versions: from 0.0.0 to 2.0.11.	3.7	More Deta
CVE-2026-107311	Improper Check for Unusual or Exceptional Conditions vulnerability in Drupal Permissions by Term allows Forceful Browsing. This issue affects Permissions by Term versions: from 0.0.0 to 3.1.41.	3.7	More Deta
CVE-2026-118776	Forge (also called node-forge) is a native implementation of Transport Layer Security in JavaScript. Prior to 1.4.1, the affected implementation used decipher.finish(), CBC and ECB modes, PKCS#7 padding to process the relevant input or security decision. node-forge validated only the final byte of PKCS#7 padding during CBC and ECB decryption and accepted zero, oversized, or mismatched padding bytes. Malformed ciphertext could consequently be accepted and up to four plaintext blocks could be silently removed, causing an integrity failure in applications that treated successful decryption as proof of valid padding. This issue is fixed in version 1.4.1.	3.7	More Deta
CVE-2026-118775	Forge (also called node-forge) is a native implementation of Transport Layer Security in JavaScript. Prior to 1.4.1, asn1.oidToDer() in lib/asn1.js did not range-check the first two arcs of an OID. An application that accepted an untrusted OID string, checked or authorized that string, and then encoded it with asn1.oidToDer() could emit DER representing a different, trusted OID from the one that was checked. DER parsing is not affected. This issue is fixed in version 1.4.1.	3.7	More Deta
CVE-2026-118774	Forge (also called node-forge) is a native implementation of Transport Layer Security in JavaScript. Prior to 1.4.1, the affected implementation used certificate.verify(child), _verifySignature(), lib/x509.js to process the relevant input or security decision. node-forge selected RSA padding and RSASSA-PSS parameters from the issuer certificate rather than the child certificate being verified. A child labeled as RSASSA-PSS could therefore be accepted with a PKCS#1 v1.5 signature when the issuer used PKCS#1 v1.5. The signature still had to be produced with the trusted issuer's private key, so this did not permit certificate identity forgery, but it could bypass policies that require a declared signature scheme. This issue is fixed in version 1.4.1.	3.7	More Deta
CVE-2026-118372	LibreSSL ocspcheck through 4.4.0 contains a CRLF injection vulnerability that allows attackers to inject HTTP headers by embedding CR/LF sequences in a certificate's AIA OCSP URI path. Because url2host() copies the path without rejecting control characters and http_open() places it in the POST request line, attackers can inject headers or split OCSP requests sent to the responder host.	3.7	More Deta
CVE-2026-108685	The WP Post Author WordPress plugin before 4.2.0 does not check that the account was created before updating its profile during front-end registration, allowing unauthenticated users to overwrite the display name, nickname and website of the first user account, which is normally the administrator, when a registration form declares one of those fields.	3.7	More Deta
CVE-2026-115456	A flaw was found in gcc. An attacker could cause a Denial of Service (DoS) by passing a string that is not null-terminated to the std::from_chars() function in the libstdc++ library. This issue triggers an out-of-bounds read beyond the allocated buffer, potentially leading to invalid data parsing or an application crash.	3.7	More Deta
CVE-2026-108686	The WP Post Author WordPress plugin before 4.2.0 does not restrict the integration settings it returns to visitors, allowing unauthenticated users to read the reCAPTCHA secret key when one has been saved.	3.7	More Deta
CVE-2026-118475	A flaw was found in Eye of GNOME. When parsing a specially crafted PNG image containing malformed color profile metadata, the application fails to validate chunk boundaries while searching for a null terminator. An attacker could trick a user into opening a malicious image, causing the application to read past the allocated buffer. This issue can lead to an application crash, resulting in a Denial of Service (DoS), or potentially expose sensitive memory contents.	3.6	More Deta
CVE-2024-3586	The LetterPress WordPress plugin before 2.4.0 does not sanitise and escape some of its settings, 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 multisite setup)	3.5	More Deta
CVE-2026-118585	A vulnerability was identified in configuroweb inventariobasico c9377cdba474deb3eb5a0704d197b5733af16b47/f9db0c0a04d79ad931c218140df4fb23809d4fab. This vulnerability affects unknown code of the file addlist.php of the component Add Product Page. Such manipulation of the argument product name leads to cross site scripting. The attack may be launched remotely. The exploit is publicly available and might 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.	3.5	More Deta
CVE-2026-105258	The Appointment Booking Plugin WordPress plugin before 5.7.6 does not escape several booking-form step content settings before rendering them on the public booking form, allowing high-privilege users such as administrators to inject JavaScript that executes in the browser of any visitor who loads the form; on multisite, where administrators do not hold the unfiltered_html capability, this crosses a privilege boundary to unauthenticated visitors.	3.5	More Deta
CVE-2026-114555	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Data field allows Stored XSS. This issue affects Data field versions: from 0.0.0 to 2.0.14.	3.5	More Deta

CVE-2026-104312	IBM Langflow OSS 1.0.0 through 1.12.3 could allow an authenticated attacker to produce a server-generated ZIP archive containing entry paths that traverse outside the intended extraction directory. Extraction of the archive by a victim using a non-sanitizing tool could result in arbitrary file write on the victim's host.	3.5	More Deta
CVE-2026-85498	A flaw was found in polkit. When processing input that begins with a null byte, an arithmetic error in the authentication agent helper causes an integer underflow during buffer length calculation, resulting in an out-of-bounds memory read. An attacker capable of supplying crafted input can trigger this flaw, potentially causing an application crash and resulting in a Denial of Service (DoS).	3.5	More Deta
CVE-2026-119330	Immich is a high-performance self-hosted photo and video management solution. Prior to 3.2.0, the shared-link creation API accepted albumId and assetIds as independent fields in server/src/services/shared-link.service.ts but authorized only the resource selected by the requested link type. An authenticated attacker who already knew a victim-owned asset UUID could select SharedLinkType.Album for an attacker-owned album while supplying that UUID in assetIds; SharedLinkService.create() persisted the unchecked association in shared_link_asset and made the victim asset available through the new anonymous shared-link credential. This exposed victim metadata, thumbnails, and the byte-identical original file and created a persistent sharing relationship that could be redistributed. This issue is fixed in version 3.2.0.	3.5	More Deta
CVE-2026-118276	A vulnerability was determined in a2ui-project a2ui up to 0.10.6. This vulnerability affects the function formatString of the file renderers/web_core/src/v0_9/basic_catalog/expressions/expression_parser.ts of the component Parser. This manipulation causes resource consumption. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized. Patch name: 1f71d1aac1b145ef57c7526f9e0cff316f5934e2. Applying a patch is the recommended action to fix this issue.	3.5	More Deta
CVE-2026-105615	PostgreSQL's optimized statistics on a table are visible as long as you have SELECT privilege on said table. A masked role can therefore read a limited subset of the data through the statistics view's histograms and mcvs. The vulnerability is resolved in PostgreSQL Anonymizer 3.3.0 and later versions.	3.5	More Deta
CVE-2026-119550	Jellyfin through 12.4 contains an information disclosure vulnerability in PlaylistsController.GetPlaylist that allows authenticated users to read hidden item IDs by requesting public or shared playlists. Restricted or parental-controlled users can obtain GUIDs of inaccessible library items from unfiltered playlist ItemIds and then stream that hidden media.	3.5	More Deta
CVE-2026-105612	PostgreSQL Anonymizer contains a vulnerability that data-modifying CTEs to bypass the read-only restriction of masked roles. The problem is resolved in PostgreSQL Anonymizer 3.3.0 and later versions	3.5	More Deta
CVE-2026-90721	Dell PowerProtect Data Domain, Feature Release versions 7.7.1.0 through 8.8, LTS2024 release versions 7.13.1.0 through 7.13.1.80, LTS2025 release versions 8.3.1.0 through 8.3.1.40, LTS2026 release versions 8.6.1.0 through 8.6.1.20, contain a Path Traversal vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Denial of service.	3.4	More Deta
CVE-2026-54610	LibreDWG is a free C library to read and write DWG files. Prior to 0.14, `bit_TV_to_utf8()` in `src/bits.c` can write to the caller-provided `src` buffer despite accepting const input. On an `iconv()` error other than `E2BIG`, the function frees its output buffer and passes the original input alias to `bit_u_expand()`, which expands or shrinks Unicode and multibyte escape sequences in place. If the input is a string literal, read-only mapping, or other immutable buffer, the write can cause a segmentation fault and denial of service; mutable caller-owned input can be unexpectedly modified before being returned. This affects applications that expose the conversion API to untrusted input under those conditions. Direct file-triggered exploitability through normal DWG decode/export paths remains unconfirmed because many TV strings are heap allocated by bit_read_TV(). This issue is fixed in version 0.14.	3.3	More Deta
CVE-2026-119124	ImageMagick before 7.1.2-34 contains a heap-based buffer overflow in its -morph processing, where crafted images cause writes beyond the bounds of a heap buffer. An attacker can supply a crafted image that, when processed by a user with the -morph option, corrupts heap memory and crashes the application.	3.3	More Deta
CVE-2026-112922	A flaw was found in Ghostscript. A remote attacker could exploit this vulnerability by enticing a user to process a specially crafted PDF or PostScript document containing malicious mesh shading data. Due to improper bounds validation during the processing of indexed color values, Ghostscript triggers an out-of-bounds memory read. Successful exploitation can lead to a Denial of Service (DoS) through an application crash or result in limited information disclosure.	3.3	More Deta
CVE-2026-119558	OpenCart through 4.1.0.4 contains a business logic vulnerability that allows logged-in customers to place unpaid full-price orders by clearing reward points after selecting Free Checkout. Attackers can apply points, save Free Checkout, then submit zero points via reward.save so the confirm handler advances the order to Free Checkout status without payment.	3.1	More Deta
CVE-2026-119126	Parse Server before 8.6.106 and 9.0.0 before 9.10.5-alpha.7 mishandles dot notation keys with null or undefined values when building the saved object, so a write is stored but returns an error and skips afterSave triggers and LiveQuery events. A client with write access can exploit this to evade audit logging, notifications, and derived data updates.	3.1	More Deta
CVE-2026-119567	vsftpd through 3.0.5 contains an access control bypass vulnerability that allows authenticated FTP users to execute denied commands by issuing RFC 775 X-prefixed aliases. The cmds_denied check in process_post_login() compares literal tokens, so attackers can send XRMD, XMKD, XCWD, XPWD, or XCUP to perform blocked operations like deleting directories.	3.1	More Deta
CVE-2026-100355	Campfire is a web-based chat application. In version 1.4.4 and earlier, when a Campfire message contains a link, the server fetches it to build an OpenGraph unfurl preview. `RestrictedHTTP::PrivateNetworkGuard` relied on Ruby's `IPAddr#private? `` IPAddr#loopback?`, and `IPAddr#link_local?` predicates plus IPv4-mapped and IPv4-compatible checks, which do not cover several special-use ranges. An authenticated user can post a link to a hostname resolving to CGNAT `100.64.0.0/10`, NAT64 `64:ff9b::/96` or `64:ff9b:1::/48`, or 6to4 `2002::/16` to bypass the guard and cause server-side requests to internal network resources. The NAT64 and 6to4 ranges can embed an internal IPv4 target. Confidentiality impact is limited to returned OpenGraph metadata, and most internal endpoints return none. There is no integrity or availability impact. An initial fix was released in version 1.4.5.	3.1	More Deta
CVE-2026-3583	When the `allowed_scopes` configuration is enabled, the OAuth2 token introspection mechanism does not immediately invalidate a token in the cache after a revocation request. This results in a scenario where an access token that was introspected immediately before a revocation request may be returned again to the client after revocation, until the relevant cache entry is cleared. The security consequence is that a revoked access token may be re-issued to the client during the cache lifetime. While the re-issued token is not treated as valid for API authorization, affected users may be unable to obtain a new valid access token until the cache is cleared, which can disrupt authentication flows.	3.1	More Deta
CVE-2026-119548	Lago through 1.55.0 contains an authorization bypass vulnerability in Invoices::Payments::StripeService that allows users of one organization to mark another organization's invoice as paid due to an unscoped invoice lookup. Attackers controlling their organization's Stripe integration can sign a payment_intent.succeeded event carrying a victim invoice UUID to unlock wallet top-ups or payment-gated subscriptions.	3.1	More Deta
CVE-2026-107308	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Country allows Cross-Site Scripting (XSS). This issue affects Country versions: from 0.0.0 to 2.1.3, from 2.2.0 to 2.2.1.	3.1	More Deta

CVE-2026-119570	Parse Server from 9.7.0 before 9.10.5-alpha.7 contains an information disclosure vulnerability that allows clients to receive protected field values written by beforeSave triggers using dot notation keys. When protectedFieldsSaveResponseExempt is set to false, clients with create or update permission can read values a trigger writes beneath a protected field in the same request.	3.1	More Deta
CVE-2026-119125	Parse Server before 8.6.107 and 9.0.0 before 9.10.5-alpha.8 returns the stored value of a field reverted by a beforeSave trigger in object update responses, even to clients without read access to that object or field. An authenticated client able to update an object whose beforeSave trigger reverts a field, via revert() or a constant: true validator, can read protected values, including its own account's raw MFA authData when protectedFieldsTriggerExempt is enabled.	3.1	More Deta
CVE-2026-118781	Forge (also called node-forge) is a native implementation of Transport Layer Security in JavaScript. Prior to 1.4.1, the affected implementation used BigInteger.prototype.modInverse(), bnModInverse(), lib/jsbn.js, RSA public exponent e to process the relevant input or security decision. node-forge's bundled jsbn implementation entered an infinite loop when BigInteger.prototype.modInverse() received a negative value or modulus. An attacker who could control the RSA public exponent passed to key generation, or a direct modInverse() operand, could block the Node.js event loop at full CPU. Parsed DER, PEM, JWK, PKCS#12, X.509, and TLS values are unsigned and cannot trigger this issue. This issue is fixed in version 1.4.1.	2.9	More Deta
CVE-2026-113494	The GeoDirectory WordPress plugin before 2.8.195 does not perform any status or ownership check when rendering a listing referenced by an id attribute in its field shortcodes, allowing users with the Contributor role and above to disclose the content and custom fields of other users' draft, pending, private and trashed listings.	2.7	More Deta
CVE-2026-90723	Dell PowerProtect Data Domain Management Center, Feature Release versions 7.7.1.0 through 8.8, LTS2024 release versions 7.13.1.0 through 7.13.1.80, LTS2025 release versions 8.3.1.0 through 8.3.1.40, LTS2026 release versions 8.6.1.0 through 8.6.1.20, contain an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Information disclosure.	2.7	More Deta
CVE-2026-90724	Dell PowerProtect Data Domain Management Center, Feature Release versions 7.7.1.0 through 8.8, LTS2024 release versions 7.13.1.0 through 7.13.1.80, LTS2025 release versions 8.3.1.0 through 8.3.1.40, LTS2026 release versions 8.6.1.0 through 8.6.1.20, contain an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Information disclosure.	2.7	More Deta
CVE-2026-90719	Dell PowerProtect Data Domain Management Center, Feature Release versions 7.7.1.0 through 8.8, LTS2024 release versions 7.13.1.0 through 7.13.1.80, LTS2025 release versions 8.3.1.0 through 8.3.1.40, LTS2026 release versions 8.6.1.0 through 8.6.1.20, contain an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Information disclosure.	2.7	More Deta
CVE-2026-86401	Dell PowerProtect Data Domain Management Center, Feature Release versions 7.7.1.0 through 8.8, LTS2024 release versions 7.13.1.0 through 7.13.1.80, LTS2025 release versions 8.3.1.0 through 8.3.1.40, LTS2026 release versions 8.6.1.0 through 8.6.1.20, contain an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Information exposure.	2.7	More Deta
CVE-2026-59385	A user with SpaceDeveloper privileges could modify the URL of a space-scoped broker without altering its credentials, enabling extraction of existing broker credentials by redirecting them to a broker under their control. The CF API does not permit direct reading of broker credentials, making this an indirect extraction method.	2.7	More Deta
CVE-2026-101209	Dell OpenManage Enterprise, versions prior to 4.8.0, contains a Server-Side Request Forgery (SSRF) vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Information exposure.	2.7	More Deta
CVE-2026-110507	The Page Builder by SiteOrigin WordPress plugin before 2.38.0 does not restrict the query arguments users can add to its Post Loop widget or limit the loop to posts they are allowed to read, which could allow users with the contributor role and above to read the content of other users' draft, pending, scheduled and private posts and pages.	2.7	More Deta
CVE-2026-119133	Wasmtime 47.0.0 before 48.0.6 and 49.0.0 before 49.0.3 contains a memory misalignment flaw in VMContext layout that causes undefined behavior when modules contain an odd number of exception tags. A WebAssembly module with an odd tag count misaligns subsequent host fields in embedders with exceptions enabled, although no exploitation path is currently known.	2.6	More Deta
CVE-2026-119130	Wasmtime before 36.0.18, 37.0.0 before 48.0.6, and 49.0.0 before 49.0.3 does not verify that set-path-with-query values in wasmtime-wasi-http are paths, so absolute-form URLs are written verbatim as the HTTP/1.1 request target while the connection uses the allowed authority. A malicious guest can supply an absolute URL that a forward proxy or gateway at that authority honors, reaching hosts disallowed by embedder filtering policies.	2.6	More Deta
CVE-2026-119377	SQLite before 3.54.0 contains an authorization bypass vulnerability in lookupName() that invokes the authorizer only for the first joined table's USING column. Attackers able to submit SQL can query a shared USING column in a RIGHT or FULL JOIN to read columns denied via sqlite3_set_authorizer() SQLITE_READ restrictions.	2.5	More Deta
CVE-2026-119334	Pi-hole is a DNS sinkhole that protects devices from unwanted content without installing any client-side software. Prior to 6.5, gravity.sh checks file:// adlist readability with sudo -u pihole test -r but then allows curl, sometimes running as root, to normalize URL dot segments and open a different file. A pihole-readable decoy can therefore pass the check while curl reads a root-only target, and /proc/self paths can similarly resolve against different processes. Exploitation requires an administrator who can add adlists and can place a symlink and decoy on the filesystem. This issue is fixed in version 6.5.	2.2	More Deta
CVE-2026-119341	Tesseract is an open source OCR engine. Prior to 5.5.4, ReadAdaptedClass in src/classify/adaptive.cpp raw-reads an ADAPT_CLASS_STRUCT from a pre-adapted-template .a file without neutralizing TempProtos and Config pointer fields before any destructor path. When the legacy engine is selected, classify_use_pre_adapted_templates is enabled, and an attacker can write the output-basename .a file, the success or rejection path can pass file-controlled pointers to ~ADAPT_CLASS_STRUCT and operator delete, causing memory corruption and denial of service. This issue is fixed in version 5.5.4.	0.0	More Deta
CVE-2026-61848	Crass is a Ruby CSS parser that's fully compliant with the CSS Syntax Level 3 specification. Prior to 1.0.7, when Crass parses input containing `non-ASCII characters`, inefficiencies in tracking the positions of `multi-byte characters` result in superlinear parsing time. An attacker-controlled CSS input consisting of many `non-ASCII characters` can therefore cause excessive CPU consumption and potentially denial of service. This issue is fixed in version 1.0.7.	N/A	More Deta
CVE-2026-109213	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2026-113499. Reason: This candidate is a reservation duplicate of CVE-2026-113499. Notes: All CVE users should reference CVE-2026-113499 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Deta
CVE-	CallBackery versions before 0.62.0 for Perl send users their own password hash and the admin-only user note via getUserConfig. getUserConfig() returns the caller's whole cbuser row, including the stored password hash and the note field that the user interface shows only to administrators.		

2026-118996	getTableData() and getAllFieldValues() in the user management plugins also return the note to users without the admin right. A non-administrator can read the notes administrators keep about them, and an attacker who obtains a session token can get that user's password hash and crack it offline.	N/A	More Deta
CVE-2026-104383	Improper Control of Generation of Code in Pigeon MFA service in EagleCloud Aquila versions through 2.6.7.2 on on-premises platforms allows authenticated remote attackers to execute arbitrary code via code injection	N/A	More Deta
CVE-2026-99100	In the Linux kernel, the following vulnerability has been resolved: wifi: p54: validate firmware record lengths The p54 firmware parser accesses component ID and component version records without checking that their lengths cover the fields being read. A malformed record can therefore make the parser read past the record. Validate the component ID and component version record lengths before accessing their data. The descriptor record is also checked against the shortest descriptor length found in the supported firmware images. Reject descriptor values that underflow the RX offset or produce an empty RX range before updating the driver state.	N/A	More Deta
CVE-2026-119036	Business::GoCardless versions before 1.01 for Perl allow memory exhaustion by flattening legacy webhook payloads before checking their signature. A webhook body with a top-level "payload" key is verified as a legacy webhook. To rebuild the signed string, the payload is flattened into one key and value pair per leaf, each key carrying the full path to that leaf, and the pairs are then encoded, sorted and joined. A long key holding a long array costs memory proportional to the key length times the array length. A remote attacker can exhaust memory in the process receiving webhooks with a single request that carries no valid signature.	N/A	More Deta
CVE-2026-119037	Business::GoCardless versions before 1.01 for Perl accept forged webhooks when a configured webhook secret is undef or empty. signature_valid uses each configured secret as the HMAC key, and nothing rejects undef or an empty string, both of which Digest::SHA treats as an empty key. A secret read from an unset environment variable, or an empty entry in a list of rotated secrets, is used as is. A remote attacker can sign a forged webhook with an empty key and have it accepted as sent by GoCardless.	N/A	More Deta
CVE-2026-119038	Business::GoCardless versions before 1.01 for Perl complete redirect flows without checking the session token, letting a leaked redirect flow ID create payments against another customer's mandate. confirm_resource takes no session token from the caller. It reads the redirect flow back from the GoCardless API and completes it with the token from that response, so the check that the flow is completed by the session that started it always passes. It then creates the requested payment or subscription against the flow's mandate. Since version 1.00, a flow that already has a mandate is returned as confirmed without being completed again, so the same ID creates a new payment on every call. A remote attacker who obtains another customer's redirect flow ID can create payments or subscriptions against that customer's mandate.	N/A	More Deta
CVE-2026-118994	CallBackery versions before 0.62.0 for Perl allow log injection via newlines in the login name. login() writes the login name to the application log without escaping control characters. The login RPC method needs no authentication, so a name containing a newline followed by text in the log record format adds a forged record. An unauthenticated attacker can forge log records, such as a successful administrator login from an address of their choosing.	N/A	More Deta
CVE-2026-13576	CallBackery versions before 0.62.0 for Perl store user passwords as unsalted HMAC-SHA1 hashes. Passwords are hashed with hmac_sha1_sum() from Mojo::Util with no key, a single fast SHA-1 HMAC. There is no salt, so equal passwords give equal hashes, and no work factor slows down guessing. An attacker who obtains the user table can recover passwords by fast offline guessing.	N/A	More Deta
CVE-2026-64860	Rejected reason: Further research determined the issue is not a vulnerability.	N/A	More Deta
CVE-2026-117346	Bitcoin Core through 31.1 is vulnerable to Denial of Service via undo files having no size limit	N/A	More Deta
CVE-2026-115830	In Secret Server versions earlier than 12.3.1, a user under certain conditions could submit an unsigned JWT and receive cloudadmin permissions in response.	N/A	More Deta
CVE-2026-63201	Netopeer2 is a server for implementing network configuration management based on the `NETCONF` Protocol. In affected versions, a low-privileged authenticated `NETCONF` user can remotely crash `netopeer2-server` by sending a `get RPC` with an invalid `subtree filter` whose text contains format specifiers. In `src/netconf.c`, `np2srv_rpc_get_cb()` sends the invalid value through `ERR()` to `np2log_printf()`, where `vsnprintf()` first formats the message safely. In `src/log.c`, that already formatted buffer is subsequently passed to `np2log()` as the format string itself, causing `vsyslog()` to interpret attacker-controlled percent sequences and read invalid pointer arguments. The reported denial of service was confirmed on version 2.8.7 using `NETCONF`-over-SSH and AddressSanitizer; reliable remote code execution was not confirmed. `The advisory identifies 2.8.8 as patched`; repository comparisons verify the fix in public release 2.8.21. The affected/fixed boundary remains unresolved because no public 2.8.8 tag was located, which does not establish the status of an untagged 2.8.8 build.	N/A	More Deta
CVE-2026-75882	An improper access control vulnerability in ESET Endpoint Encryption and ESET Full Disk Encryption allow attacker with standard user permissions access a device interface belonging to a privileged kernel driver and send specially crafted requests.	N/A	More Deta
CVE-2026-118995	CallBackery versions before 0.62.0 for Perl accept unintended values in form fields checked by createRxValidator. createRxValidator() is documented to anchor the supplied pattern at both ends, but builds /^${rx}$/ without grouping the pattern. An alternation such as yes|no then accepts any value starting with yes or ending with no, and $ also accepts a value with one trailing newline. An authenticated user can submit values the pattern was meant to reject, which an application may then write into generated configuration files.	N/A	More Deta
CVE-2026-118993	CallBackery versions before 0.62.0 for Perl allow denial of service via the request path interpolated as a regular expression under CGI, FastCGI and PSGI. The before_dispatch hook installed by startup() removes PATH_INFO from the end of the request URI with a substitution that interpolates PATH_INFO unquoted. Under CGI, FastCGI and PSGI both values come from the request, so the client chooses both the pattern and the string it is matched against. A short unauthenticated request with a backreference in the path backtracks exponentially and can keep a worker process busy for minutes.	N/A	More Deta
CVE-2026-111487	An out-of-bounds write vulnerability in the Qt Framework assimp scene import plugin of the Qt3D module.	N/A	More Deta
CVE-2026-118991	CallBackery versions before 0.62.0 for Perl encrypt configuration backups with the padded password as the AES key. getCrypt() pads the backup password with "x" characters and cuts it to 32 bytes to form the AES key, with no salt and no key derivation. The first block of a backup holds a 16 hex digit length field, so decrypting one block confirms a password guess at raw AES speed. An attacker who obtains a backup can recover its password by fast offline guessing, and with it every credential the backup holds.	N/A	More Deta
	CallBackery versions before 0.62.0 for Perl leave a world-readable dump of the configuration database in /tmp when taking a configuration		

CVE-2026-118990	backup. getConfigBlob() has the sqlite3 shell write the dump to /tmp/cbdump<pid> and never removes it. The file takes the process umask, and a symlink planted at that predictable name is followed. The dump holds every user's password hash and every value saved by the application's forms. A local user can read these after any backup, and may redirect the dump to a file of their choosing.	N/A	More Deta
CVE-2026-115829	In Secret Server versions earlier than 12.3.1, a user could bypass the initial login step and authenticate by successfully negotiating the second factor login step only.	N/A	More Deta
CVE-2026-118988	CallBackery versions before 0.60.1 for Perl let unauthenticated clients read the POD of any file via path traversal in the /doc route. Every CallBackery application mounts its documentation plugin at /doc, ahead of any session check. The route passes the requested name to Pod::Simple::Search->find without validation. find splits the name on "::" and joins the parts into a file path, so a name such as "..::..::..::etc::motd" escapes @INC. Any file the server process can read is reachable. Only POD is rendered, but a file with a POD directive and no "=cut" is POD to the end of the file.	N/A	More Deta
CVE-2026-116130	HTTP::Parser::XS versions before 0.18 for Perl truncate PATH_INFO at an encoded NUL byte in parse_http_request. The XS parser URL-decodes the request path and measures the result with strlen(), so PATH_INFO ends at the first byte decoded from %00. The pure-Perl backend is not affected. A remote attacker can send a path that a proxy or filter checks in full while the application routes on a shorter one.	N/A	More Deta
CVE-2026-116128	Starlet versions from 0.20 before 0.33 for Perl allow memory exhaustion via unbounded buffering when decoding chunked request bodies. The decoder adds each read to one buffer of unconsumed input. Nothing limits the length of a chunk-size line, so a line without a CRLF grows the buffer for as long as the client keeps sending, and the read timeout restarts after every read. The data of a large chunk is also held in the buffer until the whole chunk has arrived. A remote attacker can exhaust a worker's memory with a single request.	N/A	More Deta
CVE-2026-116127	Starlet versions before 0.33 for Perl send a body in responses to HEAD requests, corrupting the next response on a persistent or pipelined connection. The request method is not passed to the response writer, so whatever body the application returns for a HEAD request is sent. With Plack::Middleware::Head the body is empty, but an HTTP/1.1 response without a Content-Length header still gets the chunked encoding terminator. Responses with status 204 or 304 are also sent with their body. Pipelined GET and HEAD requests keep the connection open even when keep-alive is disabled, which is the default. A client or proxy reading the connection takes the extra bytes as the start of the next response, which may desynchronize a proxy that shares the connection across clients.	N/A	More Deta
CVE-2026-104384	Insufficiently Protected Credentials in tunnel gateway and provisioning interfaces in EagleCloud Aquila versions through 2.6.7.2 on on-premises platforms allows unauthenticated remote attackers to escalate privileges via authentication abuse to access the access keys, secret keys, and deployment secrets	N/A	More Deta
CVE-2026-115522	Exposure of Resource to Wrong Sphere (CWE-668) in FileArtifactService in Google Agent Development Kit (ADK) for Python (google-adk) versions 1.19.0 before 1.39.1 and 2.0.0a1 before 2.7.0 allows a caller in one application to list, read, overwrite, or delete artifacts belonging to another application when both applications share a FileArtifactService root directory and use the same user_id (and session_id for session-scoped artifacts). FileArtifactService accepted app_name across its public API methods but omitted app_name when constructing on-disk paths (root/users/{user_id}/... instead of root/apps/{app_name}/users/{user_id}/...). Version 2.6.0 scoped writes by app_name but retained a legacy root/users/{user_id} fallback for reads and deletes; version 2.7.0 and the 1.x backport in version 1.39.1 removed the fallback and enforce full per-app path scoping.	N/A	More Deta
CVE-2026-115866	Starlet versions from 0.20 before 0.33 for Perl allow CPU exhaustion via regular expression backtracking when decoding chunked request bodies. A chunk-size line is matched as a run of hex digits, then .* and a CRLF. A run followed by a bare LF and then a CRLF can never match, and the engine retries the match once for each digit, so the time taken grows with the square of the run length. Nothing limits the length of the run, which can span several reads. A remote attacker can occupy a worker for about a minute of CPU time with one 128 KiB request, before the application is called.	N/A	More Deta
CVE-2026-115865	Starlet versions before 0.33 for Perl allow a request declaring a large Content-Length to kill a worker by exhausting memory. The request body is read in a loop that asks sysread for all of the remaining declared length at once. Perl grows the read buffer to that size before any data arrives, so a length larger than available memory makes the worker exit with an uncatchable out of memory error before the application is called. A remote attacker can force a worker restart with each request of a few bytes.	N/A	More Deta
CVE-2026-61618	SNARK Verifier is a generic (S)NARK verifier. Prior to 0.2.5, KZG accumulator public-instance limbs are decoded without consistently enforcing canonical limb bounds before elliptic-curve coordinate reconstruction. `PlonkProof::read` selects scalars using `accumulator_indices` and passes them to `AccumulatorEncoding::from_repr`. For the EVM loader, `LimbsEncoding::from_repr` forwards them to `EvmLoader::ec_point_from_limbs` in `snark-verifier/src/loader/evm/loader.rs`, where `shl` and `add` reconstruct coordinates before `validate_ec_point` checks the resulting affine point rather than the original limb bounds. The related native path in `snark-verifier/src/pcs/kzg/accumulator.rs` can reach assertion- or unwrap-based decoding and panic instead of returning a verification error. This allows noncanonical encodings at the verifier boundary and can crash the native verifier. Standard SDK aggregation circuits are expected to constrain accumulator limbs before this boundary, which limits practical exploitability. This issue is fixed in version 0.2.5.	N/A	More Deta
CVE-2026-115828	In Secret Server versions earlier than 12.3.1, Secret Server did not always validate the PIN or biometric check when using a FIDO2-compliant device	N/A	More Deta
CVE-2026-87768	DateTime::Lite versions before 0.8.1 for Perl allow CPU exhaustion via a per-day loop when adding seconds. _normalize_leap_seconds crosses day boundaries one day at a time, so add(seconds => $n) on an object with a non-floating time zone takes about \|$n|/86400 iterations, and nothing limits $n. The XS implementation and the pure-Perl fallback both have the loop. An attacker who controls the number of seconds added can keep the process busy for as long as they choose.	N/A	More Deta
CVE-2026-63224	OpenRemote is an open-source internet-of-things platform. Prior to 1.26.0, the `datapoint export` API constructs `CSV crosstab` SQL by concatenating an `asset name` and `attribute name` into a `COPY` query that uses `crosstab` and streams `TO STDOUT`. The `asset name` enters both a double-quoted column identifier and a category query enclosed by the fixed `$cat$` delimiter. Escaping single quotes in one string context does not escape embedded double quotes in identifiers or protect that dollar-quote boundary. An authenticated user permitted to create or rename an asset and read/export datapoints for one of its attributes can store SQL metacharacters in the name and request a `crosstab` export, causing injected SELECT output to be returned in the normal ZIP/CSV response. This enables database exfiltration without direct database or filesystem access or token forgery. In a multi-tenant deployment it can expose other tenants' data if the manager's database role can read shared tables; integrity and availability effects are not established by the demonstrated read primitive. This issue is fixed in version 1.26.0.	N/A	More Deta
CVE-2026-62284	OSAC operator is a Kubernetes operator. In the affected revision identified as 8220502, the `console-proxy` `RemoteConfigResolver` parses Kubernetes Secret kubeconfig data with `clientcmd.RESTConfigFromKubeConfig` without sanitizing the resulting `rest.Config`. An attacker who can create or modify a Secret labeled `osac.openshift.io/remote-cluster-kubeconfig`: "true" in a namespace where the proxy's RoleBinding grants Secret read access can supply `users[].user.exec`. When `rest.TransportFor` builds the HTTP transport for an upstream WebSocket connection, client-go invokes that exec credential plugin, spawning an arbitrary process as the osac-`console-proxy` service account inside the pod. Attacker-controlled `clusters[].server` also enables server-side request forgery from the proxy pod. Remote and auto VM cluster modes are affected, with	N/A	More Deta

	auto the default; exclusively `local` mode does not read kubeconfig Secrets and is unaffected. The credential-plugin execution path is patched in commit 7e4222b; that patch does not address the described server-address SSRF path.		
CVE-2026-118568	Insecure Storage of Sensitive Information vulnerability in Drupal Content Sync (content-sync.io) allows Retrieve Embedded Sensitive Data. This issue affects Content Sync (content-sync.io) versions: from 0.0.0 to 3.2.2.	N/A	More Deta
CVE-2026-118555	Incorrect Authorization vulnerability in Drupal Commerce License allows Forceful Browsing. This issue affects Commerce License versions: from 0.0.0 to 3.1.1.	N/A	More Deta
CVE-2026-118556	Incorrect Authorization vulnerability in Drupal Commerce Shipping allows Forceful Browsing. This issue affects Commerce Shipping versions: from 0.0.0 to 2.16.0, from 3.0.0 to 3.0.6.	N/A	More Deta
CVE-2026-118557	Incorrect Authorization vulnerability in Drupal Commerce Shipping allows Forceful Browsing. This issue affects Commerce Shipping versions: from 0.0.0 to 2.16.0, from 3.0.0 to 3.0.6.	N/A	More Deta
CVE-2026-118558	Cross-Site Request Forgery (CSRF) vulnerability in Drupal Commerce Stripe allows Cross Site Request Forgery. This issue affects Commerce Stripe versions: from 2.0.0 to 2.2.3.	N/A	More Deta
CVE-2026-118559	Improper Verification of Cryptographic Signature vulnerability in Drupal Commerce Stripe allows Signature Spoof. This issue affects Commerce Stripe versions: from 0.0.0 to 1.4, from 2.0.0 to 2.2.3.	N/A	More Deta
CVE-2026-118560	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Commerce Stripe allows Cross-Site Scripting (XSS). This issue affects Commerce Stripe versions: from 2.0.0 to 2.2.3.	N/A	More Deta
CVE-2026-118561	External Control of File Name or Path vulnerability in Drupal Single Content Sync allows Path Traversal. This issue affects Single Content Sync versions: from 0.0.0 to 1.4.19.	N/A	More Deta
CVE-2026-118562	Deserialization of Untrusted Data vulnerability in Drupal Single Content Sync allows Object Injection. This issue affects Single Content Sync versions: from 0.0.0 to 1.4.19.	N/A	More Deta
CVE-2026-118563	Vulnerability in Drupal CacheFlush. This issue affects CacheFlush versions: *.*.	N/A	More Deta
CVE-2026-118564	Vulnerability in Drupal PayUmoney for Drupal Commerce. This issue affects PayUmoney for Drupal Commerce versions: *.*.	N/A	More Deta
CVE-2026-118565	Vulnerability in Drupal GroupEx PRO (Daxko) integration. This issue affects GroupEx PRO (Daxko) integration versions: *.*.	N/A	More Deta
CVE-2026-117350	Bitcoin Core prior to 29.5, 30.4, 31.2 and 32.1 is vulnerable to an OOM issue.	N/A	More Deta
CVE-2026-118567	Incorrect Authorization vulnerability in Drupal Bulk Update User Roles allows Forceful Browsing. This issue affects Bulk Update User Roles versions: from 0.0.0 to 1.0.5.	N/A	More Deta
CVE-2026-118986	CallBackery versions before 0.62.0 for Perl allow session cookie forgery via a signing secret generated with rand(). The secret that signs session cookies is built from two calls to the built-in rand(), which is seeded with 32 bits. The secret therefore has at most 2**32 possible values, and one signed cookie is enough to test each candidate offline. An attacker who obtains a single session cookie can recover the secret and sign cookies for any user, including an administrator.	N/A	More Deta
CVE-2026-115624	GROWI contains a missing authorization check vulnerability in its collaborative editing feature. By exploiting this vulnerability, a user with read-only permission, including a guest user, or a user in pending, suspended, or invited status may modify page drafts.	N/A	More Deta
CVE-2026-118553	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal AI (Artificial Intelligence) allows Stored XSS. This issue affects AI (Artificial Intelligence) versions: from 0.0.0 to 1.4.11, from 1.5.0 to 1.5.2.	N/A	More Deta
CVE-2026-118569	Incorrect Authorization vulnerability in Drupal Fasttoggle allows Forceful Browsing. This issue affects Fasttoggle versions: from 0.0.0 to 4.1.1.	N/A	More Deta
CVE-2026-118570	Cross-Site Request Forgery (CSRF) vulnerability in Drupal Fasttoggle allows Cross Site Request Forgery. This issue affects Fasttoggle versions: from 0.0.0 to 4.1.1.	N/A	More Deta
CVE-2026-118571	Use of Web Browser Cache Containing Sensitive Information vulnerability in Drupal Media Alias Display allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Media Alias Display versions: from 0.0.0 to 2.1.3, from 3.0.0 to 3.0.3.	N/A	More Deta
CVE-2026-118572	Authentication Bypass Using an Alternate Path or Channel vulnerability in Drupal OAuth Login - OAuth OIDC SSO allows Authentication Bypass. This issue affects OAuth Login - OAuth OIDC SSO versions: from 0.0.0 to 3.1.1.	N/A	More Deta
CVE-			

2026-118573	Missing Authorization vulnerability in Drupal OAuth2 Token Manager allows Forceful Browsing. This issue affects OAuth2 Token Manager versions: from 0.0.0 to 1.2.0.	N/A	More Deta
CVE-2026-118574	Incorrect Permission Assignment for Critical Resource vulnerability in Drupal S3 File System allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects S3 File System versions: from 0.0.0 to 3.12.0.	N/A	More Deta
CVE-2026-118575	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Signature pad widget allows Stored XSS. This issue affects Signature pad widget versions: from 0.0.0 to 1.15.0.	N/A	More Deta
CVE-2026-118576	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Stage File Proxy allows Cross-Site Scripting (XSS). This issue affects Stage File Proxy versions: from 0.0.0 to 3.1.7, from 4.0.0 to 4.0.1.	N/A	More Deta
CVE-2026-118582	Authentication Bypass Using an Alternate Path or Channel vulnerability in Drupal CAPTCHA allows Functionality Bypass. This issue affects CAPTCHA versions: from 0.0.0 to 1.18.0, from 2.0.0 to 2.0.11.	N/A	More Deta
CVE-2026-118583	Incorrect Authorization vulnerability in Drupal Field Permissions allows Forceful Browsing. This issue affects Field Permissions versions: from 0.0.0 to 1.6.0.	N/A	More Deta
CVE-2026-118584	Incorrect Authorization vulnerability in Drupal Field Permissions allows Forceful Browsing. This issue affects Field Permissions versions: from 0.0.0 to 1.6.0.	N/A	More Deta
CVE-2026-118987	CallBackery versions before 0.62.0 for Perl accept session cookies of any age sent in the X-Session-Cookie header. cookieConf() rejects a cookie older than 300 seconds only when it arrives in the xsc query parameter. The same cookie sent in the X-Session-Cookie header is accepted however old it is. A session cookie that leaks through a log, a Referer header or browser history authenticates as its user indefinitely.	N/A	More Deta
CVE-2026-49115	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Deta
CVE-2026-49116	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Deta
CVE-2026-61850	Kargo manages and automates the promotion of software artifacts. From 0.6.0 until 1.8.14, 1.9.9, and 1.10.8, two authorization flaws in the `project-scoped RBAC API` let an authenticated user with delegated permission to manage a Project's `Roles` or `ServiceAccounts` confer permissions exceeding the user's own. A user authorized to edit `Roles` can create, replace, or add rules granting permissions not held by the user; a user authorized to edit a Role's ServiceAccount can bind an identity, including the user's own, to a more powerful Role. A Kargo Role comprises a `ServiceAccount, Role, and RoleBinding` in the Project namespace. Changes are written using the API server's broadly privileged credentials after only a coarse resource-kind edit check, rather than checking each permission being conferred. This permits escalation to Project-administrator access, disclosure of `Project Secrets` and credentials, and modification or deletion of Project resources. Stolen Git, container-registry, or Helm-registry credentials can extend confidentiality and integrity impacts to those external systems. Escalation remains limited to Projects where the attacker already has RBAC-management delegation and does not itself grant cluster-wide or cross-Project access. Default non-administrator roles do not permit these operations; exploitation requires an `administrator-created custom role` granting the relevant permissions and control of an account assigned that role. This issue is fixed in versions 1.8.14, 1.9.9, and 1.10.8.	N/A	More Deta
CVE-2026-62301	MyTube is a self-hosted downloader and player for several video websites. Prior to version 1.10.3, backend video access does not enforce the visitor role's intended public-only restriction when `loginEnabled=true` and a visitor password is configured. The frontend filter in `VideoContext.tsx` is only client-side, `roleBasedAuthMiddleware.ts` allows all visitor GET requests, and `storageService/videos.ts` performs `getVideos()` and `getVideoById(id)` queries without checking the caller's role or `visibility`. A visitor can enumerate `/api/videos` or request `/api/videos/:id` to retrieve hidden `visibility`=0 records, exposing titles, `sourceUrl` values, `videoPath` values, subtitle paths and `thumbnailPath` values. The `serveMountVideo()` path also serves mounted video files without `visibility` checks. Leaked paths work against unauthenticated `/videos/*` and `/subtitles/*` routes, allowing media downloads without credentials. The RSS visitor feed already filters `visibility`=1 content and is not the affected query path. Default loginEnabled=false single-user deployments are unaffected by this role-boundary issue because all callers are owner-equivalent. This issue is fixed in version 1.10.3.	N/A	More Deta
CVE-2026-22114	HTTP basic auth enforces no retry limit or backoff. Combined with the default service password, the keyspace is exhaustible.	N/A	More Deta
CVE-2026-61847	Crass is a Ruby CSS parser that's fully compliant with the CSS Syntax Level 3 specification. Prior to 1.0.7, when the `:preserve_comments` option is not enabled, which is the default, Crass discards CSS comments by recursively consuming the next token. An attacker-provided stylesheet containing a very large number of adjacent comments can cause excessive recursion and trigger a `SystemStackError`, denying service to the parsing application. Preserving comments avoids this recursive path. This issue is fixed in version 1.0.7.	N/A	More Deta
CVE-2026-61789	DBHub is a database MCP server for Postgres, MySQL, SQL Server, Oracle, MariaDB, SQLite. Prior to 0.22.6, read-only SQL validation can be bypassed on the MySQL and MariaDB connectors. In `src/utils/sql-parser.ts`, `scanSingleLineComment` treats every double dash as a comment start, whereas MySQL and MariaDB require following whitespace, a control character, or the end of the line. The read-only check in `src/tools/execute-sql.ts` validates split statements with `isReadOnlySQL`, but `src/connectors/mysql/index.ts` and `src/connectors/mariadb/index.ts` execute the original string with `multipleStatements` enabled. A double dash followed by a non-whitespace character can therefore hide a subsequent write or destructive DDL statement from the validator while the database interprets the dashes as minus operators and executes both statements. Anyone able to influence the assistant's SQL, including through prompt injection in content the assistant reads, can bypass read-only mode to modify or drop database data, subject to the database account's privileges. PostgreSQL is not affected by this path because its double-dash parsing agrees with the checker and its connector executes individual split statements. This issue is fixed in version 0.22.6.	N/A	More Deta
CVE-2026-105454	RT's automatic link creation for URLs in HTML ticket content does not HTML-escape the URL it places in the link. A URL crafted to break out of the link's address can add a script that runs when the ticket history is displayed, with no further action by the viewer. Anyone who can add HTML content to a ticket can plant it. That includes an unauthenticated sender of HTML email to any queue that grants CreateTicket or ReplyToTicket to Everyone, which is routine for a queue that accepts mail from the public. The script runs in the session of any user who views the ticket, and can act in RT with that user's authority. This issue was fixed in version 5.0.11 and 6.0.4	N/A	More Deta

CVE-2026-39375	Frappe Learning Management System (LMS) is a learning system that helps users structure their content. Prior to version 2.52.0, an authenticated user with a course editing role can inject malicious JavaScript through meta tag fields in the Course Management module. The values are stored without adequate HTML sanitization and are not safely escaped when rendered, allowing stored cross-site scripting. This issue is fixed in version 2.52.0.	N/A	More Deta
CVE-2026-105455	RTIR's ticket creation forms show the subject of the related ticket when splitting a ticket or creating an incident from a report, and they render that subject without HTML escaping. A ticket subject containing script runs it when a user opens either form. RTIR grants everyone the right to create Incident Reports by default, so an unauthenticated sender of an emailed report can set that subject. The script then runs in the session of the incident handler who creates an incident from the report or splits it, and can act in RT with that user's authority. The issue was fixed in version 6.0.4. RTIR 5.0 is not affected.	N/A	More Deta
CVE-2026-105456	RTIR extends RT's HTML scrubber to allow an internal link placeholder, and the extension lets through any link that merely contains the placeholder, including links using the executable javascript: scheme. The change applies to the whole RT instance once RTIR is installed, not only to RTIR's own queues. Anyone who can add HTML content to a ticket on such an instance can store such a link. That includes an unauthenticated sender of HTML email to the Incident Reports queue, which RTIR opens to everyone by default. Script runs when a user clicks the link, in that user's session, and can act in RT with that user's authority. This issue was fixed in version 5.0.11 and 6.0.4	N/A	More Deta
CVE-2026-117182	An authenticated cross-site scripting (XSS) vulnerability in the /spina/embeddable.rb component of Spina CMS v2.21.0 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted URL.	N/A	More Deta
CVE-2026-62965	SABnzbd is an open source automated Usenet download tool. Prior to 5.1.0Beta3, orphan-job management in `sabnzbd/api.py` accepts the user-controlled `value` parameter without path confinement before `os.path.join()` with `download_dir`. An absolute path discards that base directory. An attacker with a valid API key can invoke `mode=status` with `name=delete_orphan` to reach `_api_delete_orphan` and `remove_all()` in `sabnzbd/filesystem.py`, which uses `shutil.rmtree()` for recursive deletion. The advisory also identifies `_api_add_orphan` and `_api_delete_all_orphan` as affected by the path-validation issue, while its concrete arbitrary-deletion trace is through `_api_delete_orphan`. The API key is stored in plaintext in `sabnzbd.ini`. The attacker can delete files or directories writable by the SABnzbd process, including configuration, queue data, and downloads, but system files outside the regular user's ownership are not affected. This issue is fixed in version 5.1.0Beta3.	N/A	More Deta
CVE-2026-110972	Płatnik performs client-side authentication. An attacker with access to any application instance connected to the backend server can bypass the login verification process and authenticate as an arbitrary user. This issue was fixed in metric 334 in version 10.02.002.	N/A	More Deta
CVE-2026-110971	Use of a weak password encoding algorithm in Płatnik software allows a user who obtains encoded password to easily decode it. This issue was fixed in metric 334 in version 10.02.002.	N/A	More Deta
CVE-2026-112816	Improper certificate validation in the HTTPS listener in Canonical LXD 4.0.14, 5.0.10, 5.21.8, 6.9 before 4.0.15, 5.0.11, 5.21.9, 6.10.1 allows an unauthenticated attacker to authenticate as any trusted client and gain full access to the cluster and managed virtual machines via a crafted certificate chain.	N/A	More Deta
CVE-2025-49602	An issue was discovered in Keyfactor EJBCA 9. When an administrator is removed from its administrator role while having a valid TLS session, EJBCA may, in certain circumstances, cache authentication for longer than the configured maximum time (default: 30 seconds), which results in the former administrator retaining access that they should no longer have.	N/A	More Deta
CVE-2026-110970	Płatnik uses HTTP protocol to download updates, libraries and support files. It allows an attacker to conduct a Man-In-The-Middle attack, obtain transmitted data and replace the original files with their own. This issue was fixed in metric 334 in version 10.02.002.	N/A	More Deta
CVE-2026-105924	A NULL pointer dereference vulnerability in the Qt QCborValue to JSON conversion of the Qt Core module.	N/A	More Deta
CVE-2026-62968	Dream Displays provides in-game screens for streaming videos in Minecraft. From 1.5.0 until 1.8.2, user-controlled input can influence arguments passed to `yt-dlp` under specific conditions. Unintended command-line options may be interpreted by `yt-dlp`, potentially altering its behavior. This issue is fixed in version 1.8.2.	N/A	More Deta
CVE-2026-97209	Insecure Temporary File vulnerability in Mix deps.partition in Elixir allows a local user to execute code as another user via a swapped partition config file. Partitioned dependency compilation passes the project configuration to each partition VM through a file in a fixed-name directory under the shared system temporary directory, and the partition trusts what it reads back. Another local user on the same host can exploit this during a mix deps.compile run that uses partitioned compilation. Mix.Tasks.Deps.Partition.server/4 in lib/mix/lib/mix/tasks/deps.partition.ex creates the directory with File.mkdir_p/1, which accepts an existing directory without checking its owner, so a user who created it first can replace the file before client/0 reads it. This issue affects mix: from 1.20.0-rc.4 before 1.20.5.	N/A	More Deta
CVE-2026-61586	Copernik XML Factory provides secure-by-default JAXP factory creation for Java. Prior to 0.1.2, Copernik XML Factory does not block XInclude resource resolution on the stock JDK provider after an application enables XInclude on a factory returned by `XmlFactories.newDocumentBuilderFactory()` or `XmlFactories.newSAXParserFactory()`, or on an `XMLReader` passed through `XmlFactories.harden()`. An application parsing untrusted XML can resolve attacker-controlled `xi:include` references to disclose local files or, through `http` references, reach internal network endpoints by server-side request forgery. Exploitation requires use of one of those factory/hardening APIs, the stock JDK provider with Apache Xerces absent from the classpath, explicit `setXIncludeAware(true)` or the equivalent reader feature, and XML from an untrusted source. The Xerces provider selected when Xerces is present and the Android provider are unaffected. This issue is fixed in version 0.1.2.	N/A	More Deta
CVE-2026-62979	jack lets users share media libraries through their Radarr/Sonarr stack, peer-to-peer. Prior to 0.1.0, `middleware/handle-error.ts` serializes raw `FetchError` objects into HTTP responses. `lib/servers/base.ts` attaches outbound request headers on upstream non-success responses and schema-validation failures; the public `extras` field in `lib/errors/FetchError.ts` remains enumerable and is emitted by JSON serialization. These headers include the internal Radarr/Sonarr `X-Api-Key` and custom connector headers such as `CF-Access-Client-Secret`. `lib/redact.ts` redacts logs and spans but not this response path. Any client with the shared peer API key, plus Cloudflare Access credentials if required by the deployment, can force an error without a race or user interaction. `GET /peer/items/:id` and `GET /servers/health` can expose the internal media-server key, while `GET /torznab/download/:id` can expose another peer's key and Cloudflare Access secrets. The /peer/search and /items routes catch these errors and are not affected. Disclosed internal keys grant full administrative control of the corresponding Radarr/Sonarr instance, crossing the intended boundary between friends' shared peer access and private backend credentials. This issue is fixed in version 0.1.0.	N/A	More Deta
CVE-2026-14467	An information disclosure vulnerability in the Forocoches comments editor that allows an attacker to obtain unauthorised user information by inserting an image containing a malicious external URL into a comment. When a victim views the discussion thread, their browser automatically sends an HTTP/HTTPS request to the server controlled by the attacker, who can then collect information such as the source IP address, the User-Agent header, the date and time of access, and other metadata derived from the request, thereby compromising the user's privacy.	N/A	More Deta

CVE-2025-68395	ARKETEAM Protectel modules PROTECTELMAJ and BDF contain a note editor module vulnerable to Stored XSS. A low privileged attacker can inject arbitrary HTML and JS into notes, which will be rendered/executed when a user visits this module. This issue has been fixed in: PROTECTELMAJ v6.5.19 and BDF v6.4.67	N/A	More Deta
CVE-2026-119717	Rejected reason: This CVE ID has been rejected as a duplicate.	N/A	More Deta
CVE-2026-55613	uhttpd is a small HTTP server. In unpatched repository snapshots, `uh_ubus_data_send()` in `ubus.c` can desynchronize HTTP request boundaries when a `POST /ubus` JSON body arrives in multiple TCP segments. An initial segment completing a JSON object sets `du->jsobj`; a later segment takes the existing-object parse-error path and returns zero bytes consumed. The caller neither drains the remaining declared `Content-Length` nor sets `connection_close`. An HTTP request embedded in the unread body suffix is consequently processed as a new request on the same keep-alive connection. The reported reproducer returned a JSON-RPC parse error followed by a second HTTP response. This application-layer body-handler flaw is distinct from Transfer-Encoding header case handling and chunk-length state reset, and affects deployments enabling ubus, including the default OpenWrt configuration and potential proxy/CDN deployments. Repository patches 7b1bec45826bd78c8afc993435bdc0f1df2fe399 and b2285de129b9adc8b12f84f9a27c16c21f2b57a5 address this issue.	N/A	More Deta
CVE-2025-68394	ARKETEAM Protectel modules PROTECTELMAJ and BDF are vulnerable to SQL injection vulnerability. Improper neutralization of input provided by a low privileged user into "profilInput" parameter allows for SQL Injection attacks. This issue has been fixed in: PROTECTELMAJ v6.5.19 and BDF v6.4.67	N/A	More Deta
CVE-2026-116366	An issue has been discovered in ClickHouse Server that, under certain conditions, could allow an unauthenticated user with network access to execute arbitrary code on the ClickHouse Server.	N/A	More Deta
CVE-2025-68393	ARKETEAM Protectel modules PROTECTELMAJ and BDF are vulnerable to SQL injection vulnerability. Improper neutralization of input provided by a low privileged user into "Utilisateur" parameter allows for SQL Injection attacks. This issue has been fixed in: PROTECTELMAJ v6.5.19 and BDF v6.4.67	N/A	More Deta
CVE-2026-22105	Delta UFC500 charging stations derive the default credentials of the Service account from character positions of the device serial number. An unauthenticated attacker with adjacent network access can reconstruct the resulting password, or exhaust the keyspace, and log in to read and change sensitive settings such as the OCPP backend.	N/A	More Deta
CVE-2026-22109	The shipped WebUI template database retains the factory default passwords for all five account types in cleartext. Defaults are identical across devices and were unchanged on the tested unit.	N/A	More Deta
CVE-2026-22110	The web server does not check authentication on POST or PUT. An unauthenticated attacker can reboot the charger; by brute-forcing the configid, they can also set the service password and then change any setting.	N/A	More Deta
CVE-2025-68392	ARKETEAM Protectel modules PROTECTELMAJ and BDF allow low privileged users to use some of the functionalities reserved for admin users by forging direct requests to a specific endpoint. This issue has been fixed in: PROTECTELMAJ v6.5.19 and BDF v6.4.67	N/A	More Deta
CVE-2025-68391	ARKETEAM Protectel modules PROTECTELMAJ and BDF are vulnerable to arbitrary file upload. Any user is able to upload arbitrary file and override existing files in a temporary folder. This vulnerability might lead to execution of embedded JavaScript scripts when an authenticated user tries to download the uploaded file. This issue has been fixed in: PROTECTELMAJ v6.5.19 and BDF v6.4.67	N/A	More Deta
CVE-2026-85268	A Cross-Site Scripting (XSS) (CWE-79) vulnerability in the auth/handler in Google Cloud Identity Platform and Firebase Authentication versions prior to 2026-08-14 on iOS allows an unauthenticated remote attacker to execute arbitrary JavaScript using a malicious iOS bundle ID.	N/A	More Deta
CVE-2026-61803	Frappe Learning Management System (LMS) is a learning system that helps users structure their content. Prior to version 2.52.1, the `course/certificate checkout` flow accepts client-controlled pricing, allowing an authenticated user to complete a paid-course or certificate purchase for an amount other than the actual price. This is a business-logic integrity issue; it does not expose other users' data or grant elevated privileges. This issue is fixed in version 2.52.1.	N/A	More Deta
CVE-2026-61846	Crass is a Ruby CSS parser that's fully compliant with the CSS Syntax Level 3 specification. Prior to 1.0.7, Crass recursively parses `CSS simple blocks and functions` without a depth guard. An attacker-controlled CSS value containing deeply nested blocks or functions can recurse until Ruby raises `SystemStackError`: stack level too deep, or cause excessive memory usage. Version 1.0.7 adds a configurable depth limit with a conservative default. This issue is fixed in version 1.0.7.	N/A	More Deta
CVE-2026-61805	Frappe Learning Management System (LMS) is a learning system that helps users structure their content. Prior to version 2.54.0, quiz submission records are not adequately authorized on the server. Through a `REST` bypass, an authenticated student can record a passing or perfect quiz result without their answers being verified, unlocking course completion and certificates. The student can also create a submission attributed to another user, exhausting that user's allowed attempts and blocking legitimate submissions. These integrity and availability issues are scoped to quiz results; they do not expose other users' data or grant elevated roles. This issue is fixed in version 2.54.0.	N/A	More Deta
CVE-2026-55614	uhttpd is a small HTTP server. In unpatched repository snapshots, `client_parse_header()` in `client.c` lowercases header names but compares the `Transfer-Encoding` value to `chunked` using case-sensitive `strcmp`. A mixed-case transfer-coding token is accepted without enabling `r->transfer_chunked`, despite transfer-coding tokens being case-insensitive. On a keep-alive connection, the `chunked` POST body is left unread and request-shaped body bytes are parsed as another HTTP request, permitting HTTP request smuggling and boundary desynchronization. Commits ae015e099986ceace44975cb69629841a2d58d37 and 6641b050e5f7c7fd9ae92e8e119d6d6dfc6e9837 patch the issue.	N/A	More Deta
CVE-2026-61840	Quest Bot is an opensource Discord Bot. Prior to 1.1.9, the `image to GIF` command uses a request helper that validates a hostname's public IP addresses but then sends the actual request by hostname, causing a `second DNS lookup`. An attacker controlling a domain can return a public address during validation and an internal address during the connection, bypassing the internal-address protection through `DNS rebinding`. The command takes its address directly from user input and its developer-only gate is disabled in normal deployments, so any member of a server with the bot can trigger the flaw without special permissions. Requests are restricted to `HTTPS on port 443`, and content is returned only when the response is a `genuine image`. The impact is therefore mostly blind internal probing with limited retrieval of image responses from loopback or internal endpoints, not arbitrary internal-data disclosure. Common cloud metadata services using plain HTTP on another port are not reachable through this path. This issue is fixed in version 1.1.9.	N/A	More Deta
	MyTube is a self-hosted downloader and player for several video websites. Prior to version 1.10.3, `server.ts` calls `registerStaticRoutes` and `registerCloudRoutes` before `registerApiRoutes`, where `authMiddleware` and `roleBasedAuthMiddleware` are mounted. Because Express processes middleware in registration order, `staticRoutes.ts` and `cloudRoutes.ts` remain outside the authentication stack even when		

CVE-2026-62302	`loginEnabled=true`. Unauthenticated clients can access local videos through `/videos/*`, thumbnails through `/images/*` and `/images-small/*`, avatars through `/avatars/*`, subtitles through `/subtitles/*`, cloud thumbnail caches through `/api/cloud/thumbnail-cache/*`, and cloud signed URLs or redirects through `/cloud/videos/:filename` and `/cloud/images/:filename`. The frontend login wall does not protect direct media requests. Cloud routes return 404 when cloud storage is unconfigured, but that is not an authentication rejection; protected API routes correctly return 401. Combined with hidden-video path leaks, the flaw permits unauthenticated downloads of hidden media. Default loginEnabled=false single-user deployments have no authentication boundary to bypass. This issue is fixed in version 1.10.3.	N/A	More Deta
CVE-2026-62333	OpenVM is a performant and modular zkVM framework built for customization and extensibility. Before 1.7.0 in the 1.x line and in affected 2.0 and 2.1 prereleases, `MemoryMerkleAir` does not forbid Merkle expansion rows at `parent_height` = 0 or below while `expand_direction` != 0. A malicious prover can fabricate a subtree below a memory leaf and swap digests inside that subtree to change the committed memory root without a corresponding memory operation. The fraudulent rows still balance against the Merkle and compression buses and require no memory-bus operation for the changed leaf. Because the memory Merkle root binds VM memory state across continuation segment boundaries, this affects the soundness of OpenVM proofs using persistent memory. This issue is fixed in versions 1.7.0, 2.0.0-rc.3 and 2.1.0-preview.	N/A	More Deta
CVE-2026-62334	OpenVM is a performant and modular zkVM framework built for customization and extensibility. Before 1.7.0 in the 1.x line and in affected 2.0 and 2.1 prereleases, `OpenVmHalo2Verifier.verify` constructs raw proof calldata from user-controlled `proofData`, performs a `staticcall` to `address(this)`, and treats a successful call as proof acceptance. If the first four proof bytes match another external selector exposed by the wrapper, dispatch can invoke a successful non-verifier function instead of the generated Halo2 fallback verifier. Applications using the generated Solidity wrapper can consequently accept arbitrary app commitments and public values without checking the proof suffix, accumulator, app commitments or public values. This issue is fixed in versions 1.7.0, 2.0.0-rc.3 and 2.1.0-preview.	N/A	More Deta
CVE-2026-62335	OpenVM is a performant and modular zkVM framework built for customization and extensibility. Before 1.7.0 in the 1.x line and in affected 2.0 and 2.1 prereleases, `OpenVmHalo2Verifier.verify` accepts `appExeCommit` and `appVmCommit` as `bytes32` values without checking that either is less than the `BN254` scalar field modulus. Although public-value and proof-data lengths are checked, callers can provide non-canonical 256-bit encodings greater than or equal to that modulus at the Solidity wrapper boundary. Applications relying on the wrapper can therefore accept non-canonical app executable and app VM commitments, creating ambiguity between the supplied byte-level values and the field elements used by the verifier. This issue is fixed in versions 1.7.0, 2.0.0-rc.3 and 2.1.0-preview.	N/A	More Deta
CVE-2026-62337	SNARK Verifier is a generic (S)NARK verifier. Prior to 0.2.5, the Halo 2 aggregation circuit can mishandle proof points encoded as the point at infinity. `EcPointLoader::multi_scalar_multiplication` places a `Value::Assigned(_)` base paired with `Value::Constant(ONE)` into its unscaled variable-base list and passes it directly to `sum_with_const`. The default shim delegates to halo2-lib `EccChip::sum`, whose incomplete affine addition assumes nonidentity input points. A prover-controlled proof point encoded as `(0, 0)` can therefore enter the final aggregation sum through the scalar-one shortcut and affect the MSM or accumulator computation. Practical exploitability depends on the surrounding aggregation and final-decider checks; the advisory does not establish universal acceptance of invalid proofs. This issue is fixed in version 0.2.5.	N/A	More Deta
CVE-2026-95673	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2026-92243. Reason: This candidate is a reservation duplicate of CVE-2026-92243. Notes: All CVE users should reference CVE-2026-92243 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Deta
CVE-2026-117645	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in phoenixframework phoenix_html allows an attacker who controls attribute names to inject attributes and script into rendered HTML via Phoenix.HTML.attributes_escape/1. attributes_escape/1 in lib/phoenix_html.ex escapes attribute values but not attribute names. key_escape/1 passes a binary key through html_escape, which neutralizes quotes and angle brackets but not whitespace, so a key such as x onmouseover ends the attribute and starts a new one. An atom key is only dasherized, so any character passes, including quotes and >. Nested data, aria and phx keys take the same paths. An application is affected when it builds attribute keys from untrusted input and renders them through HEEx <tag {@attrs}>, content_tag/3, or a direct call. Before 3.0.0 the same code lived in Phoenix.HTML.Tag. This issue affects phoenix_html: from 1.0.0 before 3.3.5 and from 4.0.0 before 4.4.0.	N/A	More Deta
CVE-2026-73322	Incorrect Authorization vulnerability in the single-stage query engine of Apache Pinot. When broker access control is enabled, the single-stage query engine authorizes only the table named in the query's FROM clause. The lookup() transform function identifies its dimension table with a string literal argument rather than through the FROM clause, so that table was never included in the authorization check. An authenticated user who is authorized for at least one table can therefore read columns from any dimension table in the cluster, including tables they have no access to, and can retrieve arbitrary rows of it by supplying primary key values directly. Per-principal row-level security filters configured on the dimension table are likewise not applied. The multi-stage query engine is not affected. This issue affects Apache Pinot: through 1.5.1 Users are recommended to upgrade to version 1.6.0, which fixes this issue.	N/A	More Deta
CVE-2026-62347	Element Call is a native Matrix video conferencing application. From 0.16.0 until 0.20.3, the standalone Element Call `SPA` logs the `password` URL query parameter. When a user submits an error report, called a rageshake, these logs are shared with the application operator. Users can therefore unintentionally disclose the shared `password` used to encrypt the call, potentially compromising call confidentiality. Avoiding submission of bug reports or debug logs prevents this disclosure path in affected versions. Upgrading does not remove secrets from previously collected `rageshakes`, which require separate cleanup by the log-server operator. This issue is fixed in version 0.20.3.	N/A	More Deta
CVE-2026-117666	Improper Validation of Certificate with Host Mismatch vulnerability in deadtrickster ssl_verify_fun allows an adversary in the middle to impersonate a TLS peer via a certificate that carries a partial-label wildcard. try_match_wildcard/4 in src/ssl_verify_hostname.erl anchors only the text before and after the * of an identifier such as f*.example.net, so the wildcard also consumes dots and the certificate is accepted for f.evil.example.net. RFC 6125 confines a wildcard to the left-most label. The same matcher lets *.168.1.1 match the IP literal 192.168.1.1. Whole-label wildcards are matched correctly. Erlang/OTP 20.0 and later check the hostname in ssl before a user verify_fun sees valid_peer, so a client that keeps server_name_indication set rejects the mismatch regardless. Exposed are clients that disable SNI, servers that verify client certificate hostnames with this library, and direct callers of verify_cert_hostname/2. This issue affects ssl_verify_fun: from 1.0.1 before 1.1.8.	N/A	More Deta
CVE-2026-119338	Tesseract is an open source OCR engine. From 5.4.0 until 5.5.4, AppendLinePolygon in src/api/pagerenderer.cpp destroys the caller-owned right-to-left Pta accumulator while receiving it by value, leaving line_top_rtl_pts and line_bottom_rtl_pts dangling. On an upright Hebrew or Arabic page at the default PAGE XML level, POLYGONFLAG with a false skewed_flag enters the vulnerable calls, while LEVELFLAG greater than zero provides an alternative gate. The calls repeatedly read and free the stale object, causing a double free and use after free and allowing corrupted coordinates to reach RecalcPolygonline. This issue is fixed in version 5.5.4.	N/A	More Deta
CVE-2026-66026	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Deta
CVE-2026-82104	In Teltonika Networks RUTOS devices running versions from 7.22 through 7.24.2 and TSWOS devices running versions 1.9 through 1.10, a vulnerability exists whereby an unauthenticated user can directly call LUA functions, bypassing validations that might be called under normal API requests. Due to those requests not following proper flows, this could lead to OS command execution. This issue affects RUT: from 7.22 through 7.24.2; RUTX: from 7.22 through 7.24.2; RUTM: from 7.22 through 7.24.2; RUTC: from 7.22 through 7.24.2; ATRM: from 7.22 through 7.24.2; TAP: from 7.22 through 7.24.2; CAP: from 7.22 through 7.24.2; OXA: from 7.22 through 7.24.2; DAP: from 7.22 through 7.24.2; TRB: from 7.22 through 7.24.2; OTD: from 7.22 through 7.24.2; EBG: from 7.22 through 7.24.2; SWM: from 1.9 through 1.10; TSW: from 1.9 through 1.10.	N/A	More Deta

CVE-2026-109821	Improper Validation of Specified Quantity in Input vulnerability in the Elixir standard library's URI module allows an attacker who supplies a URL to cause a denial of service through CPU exhaustion. URI.parse/1 converts the port component with String.to_integer/1 in split_authority/1 (lib/elixir/lib/uri.ex) without bounding its length, so a port of up to 1,262,592 decimal digits produces a bignum of that size and a longer one raises SystemLimitError. Rendering the parsed URI back to text (URI.to_string/1, inspect/1, logging, error formatting) converts the bignum with :erlang.integer_to_binary/1, which is quadratic on Erlang/OTP 27, 28 and 29.0: a 400,000-digit port renders in about 2.6 seconds and a 1 MB port in about 18 seconds. Ports above 65535 are also accepted. This issue affects elixir: from 0.5.0 before 1.18.6, from 1.19.0-rc.0 before 1.19.7, and from 1.20.0-rc.0 before 1.20.5.	N/A	More Deta
CVE-2026-115274	Improper Validation of Specified Quantity in Input vulnerability in the Elixir standard library's JSON module allows an unauthenticated attacker who supplies a JSON document to cause a denial of service through CPU and memory exhaustion. JSON.decode/1 and JSON.decode!/1 convert each integer literal with erlang:binary_to_integer/1 and do not bound its length. A literal of one million digits decodes successfully but costs 100 to 300 times as much CPU as a string of the same length, so one request body of a few megabytes holds a scheduler for about a second. A literal of more than about 1.29 million digits raises SystemLimitError. Applications generated by phx.new decode request bodies with JSON in Plug.Parsers, before routing and authentication. This issue affects elixir: from 1.18.0-rc.0 before 1.18.6, from 1.19.0-rc.0 before 1.19.7, and from 1.20.0-rc.0 before 1.20.5.	N/A	More Deta
CVE-2026-66025	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Deta
CVE-2026-109848	GROWI contains an authorization bypass vulnerability in its tag update API and the page update API due to improper use of a user-controlled key. By exploiting this vulnerability, an attacker who can log in to the product may obtain the contents of pages without the required read permission and save them to pages that the attacker can edit.	N/A	More Deta
CVE-2026-119680	A stored cross-site scripting (XSS) vulnerability exists in the chart feature of SharePoint Manager Plus (SPMP) due to improper sanitization and HTML encoding of user-controlled data. An attacker can inject malicious HTML or JavaScript into attributes used to generate charts, including users' full names, site names, or group names. The injected content is stored and subsequently executed in the context of other users' browsers when the affected charts are rendered. This vulnerability was fixed in client application build 4508.	N/A	More Deta
CVE-2026-119682	An improper access control vulnerability exists in the multi-factor authentication (MFA) functionality of ManageEngine SharePoint Manager Plus (SPMP). A low-privileged authenticated user can bypass authorization checks to read and modify MFA configuration settings, enable or disable MFA for the application, enumerate MFA-enrolled users, and delete MFA-enrolled accounts. Successful exploitation could allow an attacker to weaken authentication protections or cause a denial of service by configuring invalid MFA settings, potentially locking legitimate users out of the application. This vulnerability was fixed in build 4507. The reproduction explicitly uses build 4506.	N/A	More Deta
CVE-2026-61845	Crass is a Ruby CSS parser that's fully compliant with the CSS Syntax Level 3 specification. Prior to 1.0.7, Crass converts `CSS scientific notation` number values with unbounded exponentiation before clamping the result to `Float::MAX`. Applications that use Crass to parse attacker-controlled CSS strings can be forced to spend disproportionate CPU and memory parsing a tiny input, potentially resulting in a crash. This issue is fixed in version 1.0.7.	N/A	More Deta
CVE-2026-61626	libass is a portable subtitle renderer for the ASS/SSA (Advanced Substation Alpha/Substation Alpha) subtitle format. From 0.17.4 until 0.17.5, libass event pruning does not guard negative Matroska `ReadOrder` values, allowing an attacker to clear arbitrarily many bits to zero at attacker-controlled positions near the NULL pointer. Exploitation requires a malicious Matroska stream loaded through `ass_process_chunk`, enabled read-order checking, and later pruning of the malicious events. Read-order checking is enabled by default unless `ass_set_check_readorder` is called with zero; pruning must occur explicitly through `ass_prune_events` or through automatic pruning previously enabled with `ass_configure_prune`. On common systems with arithmetic right shift, 32-bit int values, the upper address region reserved to the kernel, and matching binary/kernel architecture, the expected consequence is denial of service. More extensive exploitation on uncommon systems is theoretical and strongly constrained by the target addresses, bit-clearing-only mutation, and ASLR. This issue is fixed in version 0.17.5.	N/A	More Deta
CVE-2026-61627	libass is a portable subtitle renderer for the `ASS`/SSA (Advanced Substation Alpha/Substation Alpha) subtitle format. Prior to 0.17.5, libass can overread and overwrite the glyph array in `wrap_lines_measure` while rendering malicious `ASS` content. In `wrap modes other than two`, a final line ending with a literal backslash-n sequence and otherwise consisting only of such sequences or spaces can remain after early trimming and make the line-measurement loops overshoot by one glyph. When the total text size exactly matches the allocated glyph-array capacity, the first loop reads an uninitialized 32-bit fixed-point `pos.x` value, although that value is not subsequently used. The second loop writes `pos.x` and `pos.y` beyond the array, zeroing the first and adding an attacker-controllable offset to the second. No actual exploitation beyond possible denial of service is known; broader exploitation is theoretical and constrained by the addresses, limited writes, and ASLR. This issue is fixed in version 0.17.5.	N/A	More Deta
CVE-2026-93327	A Deserialization of Untrusted Data vulnerability in the SubWorkflow task in Google Cloud Application Integration versions prior to 2026-09-11 on Google Cloud Platform allows an authenticated attacker to execute arbitrary code using a maliciously crafted serialized object. This vulnerability was patched on 11 September 2026, and no customer action is needed.	N/A	More Deta
CVE-2026-62298	mouse07410/asn1c is an ASN.1 compiler. Prior to 1.2.5, `OPEN TYPE` decoding can dereference an unallocated member pointer and crash the consuming program. `OPEN_TYPE_aper_get` in `OPEN_TYPE_aper.c`, `OPEN_TYPE_ber_get` in `OPEN_TYPE_ber.c`, `OPEN_TYPE_oer_get` in `OPEN_TYPE_oer.c`, and `OPEN_TYPE_uper_get` in `OPEN_TYPE_uper.c` share the pattern: a conditional null check on `*memb_ptr2` resets presence only when the member exists, but execution then unconditionally computes an inner value from that pointer and a member offset. If the `OPEN TYPE` member has not been allocated, the null-pointer arithmetic and subsequent read cause a segmentation fault. The advisory demonstrates UPER and APER crashes for `E2connectionUpdateAcknowledge`, notes that `E2AP` uses APER, and provides a BER reproducer; OER is also explicitly identified as affected. This issue is fixed in version 1.2.5.	N/A	More Deta
CVE-2026-62162	Hydra is a layer-two scalability solution for Cardano. Prior to 2.1.0, the `Claim` branch in `hydra-plutus/validators/deposit.ak` checks only that `datum.head_id` matches the attacker-controlled `redeemer.currencySymbol` and that the transaction is valid before the deposit deadline. It neither requires spending the Head state-token UTxO in the same transaction nor constrains outputs. After a deposit made through `POST /commit` is confirmed, any third party able to build a Cardano transaction can observe and consume the pending deposit UTxO before its deadline and redirect the assets to an arbitrary address. A standalone deposit spend invokes no Head validator, bypassing its safety checks; historical head-ID binding and the Aiken rewrite retained this missing invariant. The default deadline is three times depositPeriod, so the described attack applies to pending deposits before that deadline. This issue is fixed in version 2.1.0.	N/A	More Deta
CVE-2026-105272	GROWI contains an authorization bypass vulnerability in its page viewing and commenting functionality due to improper use of a user-controlled key. By exploiting this vulnerability, an authenticated attacker may obtain the contents and comments of pages without the required read permission.	N/A	More Deta
	Daptin is a GraphQL/JSON-API headless CMS. Prior to 0.12.26, the global `LanguageMiddleware` in `server/language.go` passes the raw `Accept-Language` header from `LanguageMiddlewareFunc` through `GetLanguagePreference` to `golang.org/x/text/language.ParseAcceptLanguage` without a size or shape filter. The guard for CVE-2022-32149 counts hyphens but not underscores, even though the internal parser normalizes underscores to hyphens. Long lists of underscore-separated language subtags longer than eight characters bypass the guard. These subtags fail		

CVE-2026-62160	the `len <= 8` length check in `golang.org/x/text/internal/language/parse.go`, causing repeated `gobble` operations to move the entire remaining buffer through `runtime.memmove`. With many invalid subtags, this repeated buffer movement takes quadratic work. Unauthenticated requests to the public landing page or `/api` can consume disproportionate CPU, with a 256 KiB header already causing seconds of processing and larger input permitted by the default 1 MiB header ceiling. `resource.CheckErr` also logs the entire invalid header, amplifying cost, while normal successful HTTP responses can conceal the denial-of-service traffic. Repeated requests can saturate server CPU. This issue is fixed in version 0.12.26.	N/A	More Deta
CVE-2026-61806	Frappe Learning Management System (LMS) is a learning system that helps users structure their content. Prior to version 2.54.2, unpublished certificate records can be retrieved and viewed by users who should not have access, rather than being limited to the certificate owner and authorized staff. This can expose certificate details belonging to other users. Access to published certificates by their identifier is intentional for third-party verification and is not affected. The issue does not allow modifying data or gaining elevated privileges. This issue is fixed in version 2.54.2.	N/A	More Deta
CVE-2026-118554	Authentication Bypass Using an Alternate Path or Channel vulnerability in Drupal OpenID Connect Client allows Authentication Bypass. This issue affects OpenID Connect Client versions: from 0.0.0 to 2.3.1.	N/A	More Deta
CVE-2026-93571	Szafir is vulnerable to Path Traversal in the uploaded filename. A man-in-the-middle attacker who can reroute update request to their server can prepare arbitrary XML file that will be saved in location chosen by attacker. This issue was fixed in version 2.0 build 708.	N/A	More Deta
CVE-2026-118552	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal AI (Artificial Intelligence) allows Cross-Site Scripting (XSS). This issue affects AI (Artificial Intelligence) versions: from 0.0.0 to 1.4.11, from 1.5.0 to 1.5.2.	N/A	More Deta
CVE-2026-47235	SimulationCraft is a tool to explore combat mechanics in World of Warcraft. In builds after release-820-01 and before the identified May 7, 2026 nightly, the `bcp_api.cpp` loop over the JSON `sockets` array uses `slot_data["sockets"].Size()` without bounding `gem_idx` by `MAX_GEM_SLOTS`, which is four in `engine/sc_enums.hpp`. The destination `gem_id` and `gem_bonus_id` arrays in `engine/item/item.hpp` have only four elements. More than four socket entries therefore write beyond `gem_id` into the adjacent `gem_bonus_id` vector storage; `bonus_list` entries can also access `gem_bonus_id` out of bounds. Corrupting a vector's `_M_start` pointer causes the `item_t` destructor to free an attacker-influenced pointer during normal cleanup. The advisory reports crashes and code execution demonstrated in a testing environment. Attack inputs can arrive through a malicious `.simc` profile with a `[[equipment]]` section, a compromised addon export, or `Battle.net API` responses modified by an attacker with a privileged network position. The fix is contained in the nightly build identified as simc-1205-01-516b5d7; no containing release tag is available.	N/A	More Deta
CVE-2026-117626	Jenkins 2.587 and earlier, LTS 2.580.1 and earlier improperly identifies file paths attempting path traversal in the file browser for workspaces and $JENKINS_HOME/userContent/, allowing attackers with Overall/Read permission to obtain the names, sizes, and last modification times of files in the $JENKINS_HOME, and attackers with Item/Workspace permission to obtain the names of jobs that have a workspace on the same agent.	N/A	More Deta
CVE-2026-117816	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-118601	Alpine iLX-F511 SSH Hard-Coded Credentials Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Alpine iLX-F511 devices. Authentication is not required to exploit this vulnerability. The specific flaw exists within the SSH service. The issue results from the use of hard-coded credentials. An attacker can leverage this vulnerability to execute code in the context of the telechips user. Was ZDI-CAN-29013.	N/A	More Deta
CVE-2026-118602	Alpine iLX-F511 Fiv.System Exposed Dangerous Method Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of Alpine iLX-F511. 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 Fiv service. The issue results from an exposed dangerous method. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of root. Was ZDI-CAN-29095.	N/A	More Deta
CVE-2026-118603	Alpine iLX-F511 vCard Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected Alpine iLX-F511 devices. User interaction is required to exploit this vulnerability in that the target must connect to a malicious Bluetooth device. The specific flaw exists within the parsing of vCard data. The issue results from the lack of proper validation of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-29017.	N/A	More Deta
CVE-2026-118604	Alpine iLX-F511 Framework Service Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows physically present attackers to execute arbitrary code on affected installations of Alpine iLX-F511 devices. Authentication is not required to exploit this vulnerability. The specific flaw exists within the framework service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-29007.	N/A	More Deta
CVE-2026-118605	Alpine iLX-F511 prh_sdp_service_search_decode Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Alpine iLX-F511 devices. An attacker must first obtain the ability to pair a malicious Bluetooth device with the target system in order to exploit this vulnerability. The specific flaw exists within the prh_sdp_service_search_decode function. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-29069.	N/A	More Deta
CVE-2026-118606	Alpine iLX-F511 Framework Service Exposed Dangerous Function Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Alpine iLX-F511 devices. Authentication is not required to exploit this vulnerability. The specific flaw exists within the framework service. The issue results from an exposed dangerous function. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-29006.	N/A	More Deta
CVE-2026-118607	Alpine iLX-F511 diagapp Command Injection Vulnerability. This vulnerability allows physically present attackers to execute arbitrary code on affected installations of Alpine iLX-F511 devices. Authentication is not required to exploit this vulnerability. The specific flaw exists within the diagapp component. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-28750.	N/A	More Deta
CVE-2026-118608	Alpine iLX-F511 libanwbtstack.so prh_rfcomm_cc_process_test Out-Of-Bounds Read Information Disclosure Vulnerability. This vulnerability allows network-adjacent attackers to disclose sensitive information on affected installations of Alpine iLX-F511 devices. An attacker must first obtain the ability to pair a malicious Bluetooth device with the target system in order to exploit this vulnerability. The specific flaw exists within the prh_rfcomm_cc_process_test function. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of root.	N/A	More Deta

	Was ZDI-CAN-29018.		
CVE-2026-118609	Alpine iLX-F511 Android Auto Connection Handler Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows physically present attackers to execute arbitrary code on affected installations of Alpine iLX-F511 devices. Authentication is not required to exploit this vulnerability. The specific flaw exists within the Android Auto connection handler. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-29016.	N/A	More Deta
CVE-2026-118610	Alpine iLX-F511 Android Auto Service Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Alpine iLX-F511 devices. Authentication is not required to exploit this vulnerability. The specific flaw exists within the Android Auto service. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-29015.	N/A	More Deta
CVE-2026-118611	Alpine iLX-F511 Bluetooth OBEX Packet Handling Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows physically present attackers to execute arbitrary code on affected installations of Alpine iLX-F511 devices. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of Bluetooth OBEX packets. 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 root. Was ZDI-CAN-29012.	N/A	More Deta
CVE-2026-118613	Ultralytics torch_load Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ultralytics. 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 torch_load function. 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-29652.	N/A	More Deta
CVE-2026-118614	Ultralytics check_det_dataset Code Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ultralytics. 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 check_det_dataset function. The issue results from the lack of proper validation of a user-supplied string before using it to execute Python code. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-30119.	N/A	More Deta
CVE-2026-118615	Ultralytics torch_safe_load Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ultralytics. 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 torch_safe_load function. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-30122.	N/A	More Deta
CVE-2026-118616	Ultralytics parse_model Code Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ultralytics. 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 parse_model function. The issue results from the lack of proper validation of a user-supplied string before using it to execute Python code. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-30123.	N/A	More Deta
CVE-2026-118617	Ultralytics load_dataset_cache_file Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ultralytics. 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 load_dataset_cache_file function. 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-30124.	N/A	More Deta
CVE-2026-118618	Ultralytics parse_model Code Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ultralytics. 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 parse_model function. The issue results from the lack of proper validation of a user-supplied string before using it to execute Python code. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-30121.	N/A	More Deta
CVE-2026-118619	Ultralytics Google Drive Download Path Traversal Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ultralytics. 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 handling of downloads from Google Drive. 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 arbitrary code in the context of the current process. Was ZDI-CAN-32376.	N/A	More Deta
CVE-2026-117815	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-83525	Incorrect operator (CWE-480) in the FetchSnapshot RPC handler in Apache Kafka from 2.8.0 before 4.2.2, and from 4.3.0 before 4.3.2 on all platforms allows an authenticated attacker with CLUSTER_ACTION privilege to cause a denial of service (controller process termination) via a crafted FetchSnapshotRequest with an empty topics array or a topic with no partitions. Users are recommended to upgrade to version 4.2.2, 4.3.2, or 4.4.0, which fix this issue. Users on unsupported branches (4.1.x and earlier) should upgrade to 4.2.2 or later.	N/A	More Deta
CVE-2026-117814	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117813	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-93524	A buffer overread in CheckKeySyms() in X.Org X Server before 21.1.25 and XWayland before 24.1.14 could be used by authenticated X clients to leak small amounts of information from X server memory or potentially crash the X server.	N/A	More Deta
CVE-2026-116131	HTTP::Body versions before 1.23_01 for Perl allow memory and temporary file exhaustion via an unlimited number of form fields and multipart parts. The urlencoded parser splits the whole body on its separators at once, creating one scalar per separator before any field is stored. This costs about 90 bytes of memory per separator byte. The multipart parser creates a temporary file for every part that carries a filename. Neither parser limits how many fields or parts a body may hold. A remote attacker can exhaust worker memory with a body made of separators, or create	N/A	More Deta

	thousands of temporary files with one request of small file parts.		
CVE-2026-116132	HTTP::Body versions before 1.23_01 for Perl leave the temporary file of an incomplete multipart upload on disk. The multipart parser creates a temporary file as soon as a file part starts, but adds it to the upload list only when the part completes. Uploads are only ever deleted from that list, by the cleanup option or by the caller, so a body that ends inside a file part leaves its temporary file where nothing can find it. A remote attacker can fill the temporary directory by repeating such requests, leaving one file behind for each.	N/A	More Deta
CVE-2026-116133	HTTP::Body versions before 1.23_01 for Perl allow CPU exhaustion via quadratic rescanning of a multipart body with a missing or malformed boundary. Before the first part, and between parts, the multipart parser searches the whole buffered body for the next boundary. On a miss it keeps everything and searches again from the start when the next chunk arrives. A body with no boundary, or with a delimiter followed by neither CRLF nor "--", is therefore rescanned on every chunk, taking time quadratic in its size. A remote attacker can exhaust worker CPU with a few such requests.	N/A	More Deta
CVE-2026-116134	HTTP::Body versions before 1.23_01 for Perl allow memory exhaustion via an unbounded multipart part header block. The multipart parser takes everything up to the first blank line after a boundary as the part's header block, with no limit on its size or number of lines. Every line is stored in the part's header hash, so a block of short lines costs about 60 bytes of memory per input byte. A remote attacker can exhaust worker memory with a single request.	N/A	More Deta
CVE-2026-117625	A missing permission check in Jenkins 2.587 and earlier, LTS 2.580.1 and earlier allows attackers with Overall/Read permission to obtain the server, port, user name, and no-proxy host list of the configured HTTP proxy.	N/A	More Deta
CVE-2026-117817	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117818	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-110985	A Kafka broker using SASL/OAUTHBEARER with the default validator (sasl.oauthbearer.jwt.validator.class=DefaultJwtValidator) selects its implementation from configuration. When sasl.oauthbearer.jwks.endpoint.url is set, the validator verifies the JWT signature. When that URL is unset (the default) and no verification key resolver is supplied, DefaultJwtValidator silently falls back to ClientJwtValidator, which does not verify the JWT signature, algorithm, or issuer - and the broker starts with no warning or error. This is the residual of CVE-2026-33557, whose fix restored signature verification only on the path where the JWKS endpoint URL is set. Impact: A broker in this state accepts any structurally valid JWT, including "alg":"none" tokens. An unauthenticated remote attacker who can reach the listener can forge a token asserting any principal - including configured superusers - and gain full access to the cluster. Only brokers that enable SASL/OAUTHBEARER validation without a JWKS endpoint URL (and without a custom verification key resolver) are affected; brokers that set the URL verify signatures and are not affected. Unlike CVE-2026-110952 (issuer/audience not enforced by default), here no signature is verified at all. Mitigation (all affected versions, no upgrade required): Set sasl.oauthbearer.jwks.endpoint.url for every listener/mechanism that uses OAuthBearerValidatorCallbackHandler, or configure a signature-verifying sasl.oauthbearer.jwt.validator.class. Resolution: From Apache Kafka 4.2.2, 4.3.1, and 4.4.0: a broker that would fall back to the non-verifying ClientJwtValidator fails to start with a ConfigException instead of running without signature verification (secure by default).	N/A	More Deta
CVE-2026-117835	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117834	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117833	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117832	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117831	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117830	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117829	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117828	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117827	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117826	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-103506	An authenticated user in Grafana can read SSO client secrets and modify instance-wide SSO settings without the required permissions (missing authorization). This affects Grafana OSS and Enterprise 13.2 installations with the experimental kubernetesSsoSettingsApi feature toggle enabled, which is disabled by default.	N/A	More Deta

CVE-2026-117825	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-110952	A Kafka broker that authenticates clients with SASL/OAUTHBEARER using the bundled JWKS-backed validator always verifies the JWT signature, but two further checks are only performed when explicitly configured: - The issuer (iss) claim is verified only when sasl.oauthbearer.expected.issuer is set. When it is unset, a validly-signed token carrying the expected audience is accepted regardless of which issuer minted it. - An audience (aud) claim is required only when sasl.oauthbearer.expected.audience is set. When it is unset, a validly-signed token that omits the aud claim is accepted. (A token that carries an aud claim is still rejected when no expected audience is configured.) Both options default to unset and have been documented as optional (Importance LOW) since KIP-768 (3.1.0). Impact: The exposure is realizable mainly in deployments whose JWKS endpoint serves signing keys for more than one issuer (a multi-tenant identity provider, an aggregated/shared JWKS, or shared signing keys): a token minted for a different issuer, or a token lacking an audience, may be accepted to authenticate — potentially as a higher-privileged principal. In a single-issuer deployment where the provider controls the iss claim and issues audience-scoped tokens, exposure is limited. The signature trust anchor remains enforced in all cases. This is distinct from CVE-2026-33557 (acceptance of unsigned/unvalidated tokens); here the signature is validated and only the issuer/audience checks are not enforced by default. Mitigation (all affected versions, no upgrade required): Set both sasl.oauthbearer.expected.issuer (to your provider's exact iss value) and sasl.oauthbearer.expected.audience (to the audience(s) your brokers expect), per listener. Brokers that set these perform exact-match issuer/audience checks and are not affected. Both have been available since 3.1.0. Resolution: - From Apache Kafka 4.4.0: a broker configured with a JWKS endpoint fails to start unless both sasl.oauthbearer.expected.issuer and sasl.oauthbearer.expected.audience are set (secure by default). Deployments that intentionally do not restrict the issuer and/or audience may opt out per axis with sasl.oauthbearer.allow.unverified.issuer=true and/or sasl.oauthbearer.allow.unverified.audience=true.	N/A	More Deta
CVE-2026-111073	The broker-side PushTelemetry API (KIP-714) validates only the compressed size of a client's metrics payload against telemetry.max.bytes (default 1 MB) before decompressing it. ClientTelemetryUtils.decompress() then decompresses the payload with no limit on the decompressed output size, growing a heap buffer until the compressed input is exhausted. A small, highly compressible payload (for example gzip-compressed zeros) can therefore expand to hundreds of megabytes of broker heap. Impact: An authenticated client can send a PushTelemetry request with a small compressed payload that decompresses to a very large size, consuming broker heap out of proportion to the request size. Repeated or concurrent requests can exhaust the broker heap and cause an OutOfMemoryError, degrading or crashing the broker; a client that targets multiple brokers can affect cluster availability. PushTelemetry is available to any authenticated client and is not gated by an ACL. Mitigation: Upgrade to Apache Kafka 4.2.2, 4.3.1, or 4.4.0. On affected versions there is no configuration that fully prevents the amplification, because telemetry.max.bytes bounds only the compressed size; lowering telemetry.max.bytes reduces the worst-case decompressed size proportionally and is a partial mitigation. Resolution: - From Apache Kafka 4.2.2, 4.3.1, and 4.4.0: ClientTelemetryUtils.decompress() enforces a maximum decompressed size equal to telemetry.max.bytes (default 1 MB). Decompression reads in bounded chunks and aborts with a TelemetryTooLargeException once the decompressed total exceeds the limit, so an over-large or highly compressible payload is rejected instead of being fully expanded in heap. The decompressed size is therefore bounded by default.	N/A	More Deta
CVE-2026-117819	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-111108	Apache Kafka's code-generated protocol readers pre-size an array's collection from the element count declared by the sender. That count is checked only against the bytes remaining in the request buffer, which assumes about one byte per element; because most elements need several bytes, a request can declare far more elements than the buffer holds and still pass. For a keyed array the reader then allocates an ImplicitLinkedHashCollection of capacity (2 * count +1), so a request of a few tens of megabytes can force a heap allocation several times larger before any element is read. The pattern is emitted into every generated reader, so it affects all Kafka API types with an array field. Impact: Request parsing happens before any authorization check. On a listener that does not require authentication (for example PLAINTEXT), an unauthenticated attacker can send a few concurrent requests that each declare a very large= array length and allocate many times their wire size in broker heap, crashing the broker with an OutOfMemoryError. The reporter demonstrated three concurrent ~90 MB ProduceRequest (v3) connections exhausting a 1 GB heap (~8x amplification). On listeners that require authentication, the attacker needs valid credentials but no specific ACL, since parsing precedes authorization.. Mitigation: Upgrade to Apache Kafka 4.2.2, 4.3.2, or 4.4.0. Until then, lowering socket.request.max.bytes and restricting network access to broker listeners reduces, but does not remove, exposure. Resolution: From Apache Kafka 4.2.2, 4.3.2, and 4.4.0: generated readers cap the initial array pre-allocation at MessageUtil.MAX_PREALLOCATED_ARRAY_CAPACITY (1000) and grow it on demand, and reject a declared array length above MessageUtil.MAX_ARRAY_LENGTH (1,000,000).	N/A	More Deta
CVE-2026-111115	Apache Kafka's code-generated readers for flexible protocol versions read a tagged-field count declared by the sender and retain a RawTaggedField object for each unknown field. That count was bounded only by the outer request frame size (socket.request.max.bytes); it was not checked against the remaining buffer bytes or capped. Because each entry can be encoded in as little as two bytes (unknown tag 0, size 0), a modest request can declare tens of millions of tagged fields and force one object allocation per declared field. Flexible request headers (header version 2, used by flexible APIs such as ApiVersions v3) are parsed this way, so the amplification applies to the request header itself. Impact: The flexible request header is parsed on the network thread before authorization, request dispatch, and request-time quota accounting. A client can send a request of a few tens of megabytes whose header declares about 20 million tagged fields, forcing roughly that many RawTaggedField allocations and exhausting broker heap or inducing process-wide GC stalls, denying broker service. Because the header is parsed for pre-authentication APIs such as ApiVersions (v3), the allocation can occur before authentication; no Kafka resource ACL or quota is required. Mitigation: Upgrade to Apache Kafka 4.2.2, 4.3.2, or 4.4.0. Until then, lowering socket.request.max.bytes and restricting network access to broker listeners reduces, but does not remove, exposure. Resolution: From Apache Kafka 4.2.2, 4.3.2, and 4.4.0: generated readers bounds-check the tagged-field count for flexible-versioned messages, rejecting a negative count, a count exceeding the remaining buffer bytes, or a count exceeding a fixed maximum (10,000), before any per-field allocation.	N/A	More Deta
CVE-2026-111496	Kafka Streams derives its stream-time clock from record timestamps. PunctuationSchedule.next() computed the next punctuation time as timestamp + (intervalsMissed + 1) * interval with no overflow check. A record with a timestamp at or near Long.MAX_VALUE advances stream time to that value, so the next stream-time punctuation overflows to a negative time. PunctuationQueue then re-queues that time and loops on it indefinitely while holding a lock, stalling the StreamThread. Impact: A single record is enough. The affected StreamThread stops processing, and because the record stays in the topic the hang returns on restart; an application whose partitions are all affected becomes unresponsive. Only the Streams application is affected, not the brokers or the cluster. Triggering it needs write access to a source topic whose topology uses stream-time punctuation, and a broker that stores the record: brokers from Apache Kafka 4.0.0 reject such a timestamp by default (log.message.timestamp.after.max.ms, one hour), so it is reachable only on older brokers or where that bound has been relaxed. Mitigation: Upgrade Kafka Streams to 4.2.2, 4.3.2, or 4.4.0. As defense in depth, keep log.message.timestamp.after.max.ms bounded on source topics and restrict write access to them. Resolution: From Apache Kafka 4.2.2, 4.3.2, and 4.4.0: the next punctuation time is computed with overflow-checked arithmetic (clamped to Long.MAX_VALUE), and a rescheduled punctuation is re-queued only when its time moves forward.	N/A	More Deta
CVE-	Several Kafka deserialization paths read a size or count field from input data and use it directly to allocate an array, collection, or byte buffer, with no check against the bytes actually available. A small crafted input can therefore declare a very large size and force a multi-gigabyte allocation. The affected paths are, in Kafka Streams, ProcessorRecordContext (header count), ChangedDeserializer (varint value length), CombinedKeySchema (foreign-key length, which could also produce a negative size), ProcessorMetadata (key length), and AssignmentInfo group-assignment decoding; and, in the clients library, ListDeserializer (used by ListSerde). Impact: An attacker can trigger the oversized allocation and raise an OutOfMemoryError that crashes the affected consumer or Kafka Streams thread; the broker and the rest of the cluster are unaffected. The		

2026-111551	reachable surface depends on the path: writing a crafted record to a Streams application's internal changelog or repartition topics, or committing crafted offset metadata to its consumer group (Streams internal paths); writing a crafted record to any topic that a consumer reads with ListSerde (ListDeserializer); or, as a member of a Streams consumer group, returning crafted assignment data when elected leader (AssignmentInfo). Because a crafted record remains in its topic, the error can recur on restart. The record size limit (max.message.bytes) does not help, because the allocation is driven by a size field rather than by the input's length. Mitigation: Upgrade to Apache Kafka 4.2.2, 4.3.2, or 4.4.0. Where authorization is enabled, restrict write access to each application's internal topics and consumer group to its own principal, and restrict who can produce to topics that are consumed with ListSerde. Resolution: From Apache Kafka 4.2.2, 4.3.2, and 4.4.0: these deserialization paths validate the declared size against the remaining input before allocating and reject input that fails the check.	N/A	More Deta
CVE-2026-112375	An authenticated Kafka principal with no authorization grants (not even ALTER_CONFIGS) can make a broker read a file or an environment variable from the broker host and return its contents. An IncrementalAlterConfigs (or AlterConfigs) request targeting a BROKER resource reaches the broker's configuration validation before any authorization check is applied to that path. Validation resolves configuration variables such as ${file:/path:key} or ${env:VAR} using a ConfigProvider named in the request, and this resolution bypasses the org.apache.kafka.automatic.config.providers allowlist that was added as the mitigation for CVE-2024-31141. An arbitrary ConfigProvider (for example FileConfigProvider or EnvVarConfigProvider) is therefore instantiated and the referenced file or environment variable is read, and a type-validation error returns the resolved content to the caller. Impact: On a cluster with an authorizer enabled, an authenticated principal with no authorization grants can read the contents of files accessible to the broker process, and the broker's environment variables, exposing credentials, keystores, or other secrets, defeating the CVE-2024-31141 allowlist. The read is bounded by the broker process's file permissions. The brokers and the cluster remain available; the issue is disclosure of file and environment- variable contents. Clusters with no authorizer configured are not affected in practice, because every principal already holds ALTER_CONFIGS there. Mitigation: Upgrade to Apache Kafka 4.2.2, 4.3.2, or 4.4.0. As defense in depth, run brokers under a least-privileged operating-system account so that sensitive files are not readable by the broker process. Resolution: From Apache Kafka 4.2.2, 4.3.2, and 4.4.0: broker configuration changes are authorized (ALTER_CONFIGS on the cluster) before the configuration is validated, and configuration- variable resolution enforces the config-providers allowlist.	N/A	More Deta
CVE-2026-114349	When a broker decodes a compressed record batch, the per-record decoder reads a declared body size from the decompressed stream and allocates a buffer of that size before validating it against the bytes available or any configured limit. The size is attacker-controlled, and the batch CRC does not constrain it, so a small (around 90-byte), CRC-valid compressed produce request can declare a body size of up to about 2 GiB and force the broker to attempt that allocation, raising OutOfMemoryError. The record size limit (max.message.bytes), the request size limit, and client/broker quotas bound only the compressed wire size, not the declared decompressed size. Impact: An authenticated principal with Write on a topic can crash broker request-handler threads (reached when a batch's codec differs from the topic's compression.type and records are re-encoded) and any consumer that fetches the record, denying service. On brokers started with -XX:+ExitOnOutOfMemoryError, a common hardening, a single crafted request terminates the broker JVM. More seriously, a crafted record is accepted at ingest and written to disk; when the log-cleaner later reads it on a compacted topic, the OutOfMemoryError (an Error, not an Exception) terminates the cleaner thread, which is not restarted. With the default of a single cleaner thread, log compaction then stops for the entire broker, including the internal __consumer_offsets and __transaction_state topics, and the condition persists across restarts until the offending record is removed. The impact is availability only; no data is disclosed or altered. Mitigation: Upgrade to Apache Kafka 4.2.2, 4.3.2, or 4.4.0, and set max.decompressed.message.bytes (at the broker and/or topic level) to a bounded value appropriate for your workload. Upgrading alone is not sufficient: for backward compatibility this configuration defaults to an effectively unlimited value (about 2 GiB), so a broker remains exposed until the limit is set. Choose a value at or slightly above the largest legitimate decompressed record your applications produce, and comfortably below the broker heap divided by the number of request-handler and cleaner threads. Until you can upgrade and configure the limit, restrict Write access to trusted producers; quotas and max.message.bytes do not mitigate this issue. Resolution: From Apache Kafka 4.2.2, 4.3.2, and 4.4.0: the broker validates a record's declared decompressed body size against max.decompressed.message.bytes before allocating, on the produce-validation, log-compaction, and timestamp-lookup paths, and rejects oversized or negative sizes with InvalidRecordException. Operators must set this configuration to a bounded value to be protected, as its default is effectively unlimited.	N/A	More Deta
CVE-2026-115644	Apache Kafka Connect contains an authentication bypass vulnerability affecting the admin REST API when admin.listeners is configured with a separate listener from the main listeners property. When operators isolate the admin REST API by explicitly configuring the "admin.listeners" property, REST extensions specified via rest.extension.classes (such as BasicAuthSecurityRestExtension) are not registered or applied to the admin resource configuration. While the primary REST API listener (configured via listeners) enforces configured authentication and authorization filters, endpoints mounted under the separate admin listener (/admin/loggers) fail to inherit or instantiate these extension filters. As a result, the admin logger endpoint accepts unauthenticated read and write requests even when security extensions are active on the main listener. Impact: An unauthenticated attacker with network access to the admin listener can: 1. Read the complete set of logger names and levels, disclosing loaded class names and which security extensions are in use. 2. Write logger levels, including with scope=cluster which propagates the change to all workers in the Connect cluster. This can be used to suppress logging (setting root to OFF) or generate excessive log output (setting root to TRACE), potentially impacting availability and observability. Mitigation: Users who cannot upgrade immediately can remove the admin.listeners configuration (or leave it unset). When unset, admin resources share the regular listener and inherit its security extensions. Resolution: From Apache Kafka 4.2.2, 4.3.2, and 4.4.0, we make sure the REST extensions specified via "rest.extension.classes" will also apply to "admin.listeners".	N/A	More Deta
CVE-2026-116593	Apache Kafka Connect has the /connector-plugins/{connector-type}/config/validate endpoint on its REST API to validate connector configurations. Apache Kafka Connect also support Configuration Providers which enable to hide the values of sensitive configuration and only resolve them at runtime. An attacker with access to the validate endpoint can use it to resolve and return plaintext values via any of the configuration providers installed on a Connect worker. Users are recommended to upgrade to version 4.2.2, 4.3.2, 4.4.0 or above, which fix this issue.	N/A	More Deta
CVE-2026-117824	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117823	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117822	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117821	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117820	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-	HTTP::Body versions before 1.23_01 for Perl drop mixed-case percent escapes from urlencoded form fields instead of decoding them. The decode table holds only the all-lowercase and all-uppercase spelling of each hex pair, while the escape pattern matches either case. An escape such as %aB finds no entry and is replaced with nothing, joining the bytes on either side. Hex digits in percent escapes are case-insensitive, and	N/A	More Deta

116135	conforming decoders return the byte. A remote attacker can send a field name or value that a conforming decoder in front of the application reads differently, so that pass%aBword reaches the application as password.		
CVE-2026-116264	MIME::Field::ParamVal versions before 5.521 for Perl allow one invalid Content-Type parameter to hide the parameters after it, including the multipart boundary. Parameter parsing stops at the first parameter whose name it cannot read, such as x:y=1 or a name containing an 8-bit byte, and drops every parameter after it. When the boundary is among them, MIME::Parser keeps the multipart body as a single undecoded part without marking the parse as ambiguous. Mail readers that skip the invalid parameter still find the boundary. A remote sender can hide an attachment from a filter that relies on ambiguous_content() while the recipient's mail client shows it.	N/A	More Deta
CVE-2026-116265	MIME::Field::ParamVal versions before 5.521 for Perl do not flag an ambiguous multipart boundary written as RFC 2231 continuations. The boundary ambiguity checks look only at a plain boundary= parameter, and a boundary split into RFC 2231 sections (boundary*0=, boundary*1= and so on) is joined after they have run. A repeated section number is concatenated rather than reported as a duplicate. From version 5.518, an encoded word or trailing whitespace in such a boundary also goes unflagged, although multipart_boundary() decodes or strips it. A remote sender can make MIME::Parser split a message on a different boundary than other mail readers, hiding an attachment from a filter that relies on ambiguous_content() while the recipient's mail client shows it.	N/A	More Deta
CVE-2026-117801	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-118261	Echo is a Go web framework. From 4.0.0 until 4.16.1, Echo v4's opt-in Decompress middleware exposes a gzip-decoded request stream without limiting its expanded size. A small compressed request can expand into a very large body when a handler reads or binds it, consuming excessive memory or CPU and allowing repeated or concurrent requests to cause denial of service. The middleware is not enabled by default, and limiting only the compressed request size does not bound the decoded size. This issue is fixed in 4.16.1.	N/A	More Deta
CVE-2026-118262	Echo is a Go web framework. From 4.15.0 until 4.16.1 and 5.4.1, Echo's Proxy middleware can retain a handler, copy goroutines, and network connections after a WebSocket client disconnects when the upstream keeps its connection open. The raw proxy waits for both copy directions without reliably closing the peer connection when one direction ends, including when a rejected upgrade response uses HTTP keep-alive. Repeated connections can accumulate resources and cause denial of service, depending on proxy-route accessibility, upstream behavior, and connection deadlines. This issue is fixed in 4.16.1 and 5.4.1.	N/A	More Deta
CVE-2026-118263	Echo is a Go web framework. From 5.0.0 until 5.4.1, Echo v5's BodyDump middleware can discard a BodyLimit overflow error for an unknown-length request when BodyDump's capture limit is below the BodyLimit threshold. BodyDump drains the remaining body while ignoring read errors and replaces it with the captured prefix, so an HTTP/1.1 chunked request can be truncated and processed successfully even though the original body exceeded the configured limit. Known-length requests rejected before BodyDump runs are unaffected, and the issue does not establish a general authentication bypass or denial of service. This issue is fixed in 5.4.1.	N/A	More Deta
CVE-2026-118264	Echo is a Go web framework. From 4.0.0 until 4.16.1 and 5.4.1, Echo's Proxy middleware selects a raw tunnel from a client WebSocket upgrade request before verifying that the configured upstream accepted the upgrade. If the upstream rejects the upgrade with an ordinary keep-alive response, later HTTP requests on the connection are sent directly to that upstream without passing through Echo's router or route-specific middleware. This can bypass authentication or authorization enforced only by Echo routes, but requires an accessible proxy route, a cooperating rejected-upgrade response, and a target without independent upstream authorization. This issue is fixed in 4.16.1 and 5.4.1.	N/A	More Deta
CVE-2026-117810	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117809	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117808	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117807	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117806	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117805	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117804	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117803	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117802	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117800	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-118256	Vue I18n is the internationalization plugin for Vue.js. From 9.0.0-beta.5 until 11.4.14 and 12.0.0-alpha.5, enabling escapeParameter, called escapeParameterHtml in the Legacy API, does not escape named interpolation values when the same translation call supplies both list and named values because escapeParams() processes only the list branch. Applications that render translations as HTML and pass untrusted named values with a list can insert attacker-controlled markup, including phishing links, forms, and layout changes, and can permit script execution when	N/A	More Deta

	combined with the srcdoc sanitizer bypass or on releases without the sanitizer. This issue is fixed in versions 11.4.14 and 12.0.0-alpha.5.		
CVE-2026-117799	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117798	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117797	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117796	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117795	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117794	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117793	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117792	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117791	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-118662	Vite is a frontend tooling framework for JavaScript. From 6.4.4 until 6.4.5, the Vite development server can evaluate server.fs.deny before stripping loader query parameters such as ?raw, ?import&raw, or ?import&url&inline. When the development server is exposed to the network and a sensitive file is inside server.fs.allow but matched by server.fs.deny, an unauthenticated attacker can append one of these queries and retrieve the denied file. This issue is fixed in version 6.4.5.	N/A	More Deta
CVE-2026-118664	decode-uri-component provides a more robust alternative to decodeURIComponent. Prior to 0.5.1, decodeUriComponent in index.js falls back to customDecodeURIComponent after native decoding throws, and the fallback collects every distinct percent-encoded run before performing a full-string regular-expression replacement for each entry. Malformed input containing many distinct runs can therefore make both the number of replacements and the scanned input length grow together, causing quadratic CPU consumption and blocking the Node.js event loop; request-body inputs can reach the demonstrated size, while ordinary URL header limits reduce the practical delay. This issue is fixed in version 0.5.1.	N/A	More Deta
CVE-2026-118665	GraphQL Tools provides utilities for building, stitching, and mocking GraphQL schemas. Prior to version 1.1.36 of the GraphQL Tools legacy WebSocket executor package, buildWSLegacyExecutor in packages/executors/legacy-ws/src/index.ts retains request.extensions.connectionParams in the closure-scoped executorConnectionParams object after cleanupWebsocket closes a connection. When one executor is reused across different authorization contexts, a later request that omits a sensitive key can send an earlier caller's Authorization or tenant value in its connection_init payload, causing the downstream server to authenticate the later caller as the earlier user. Applications that create a new executor for every request are not affected. This issue is fixed in version 1.1.36 of the GraphQL Tools legacy WebSocket executor package.	N/A	More Deta
CVE-2026-118666	GraphQL Tools provides utilities for building, stitching, and mocking GraphQL schemas. Prior to version 1.1.36 of the GraphQL Tools legacy WebSocket executor package, buildWSLegacyExecutor in packages/executors/legacy-ws/src/index.ts reuses one WebSocket and replaces its single websocket.onmessage handler whenever a new overlapping subscription starts. The handler delivers LEGACY_WS.DATA frames to the newest observer without comparing data.id with the subscription operation id, so a caller using the same executor can receive another user's authorized subscription payload while the earlier caller's stream is starved. This issue is fixed in version 1.1.36 of the GraphQL Tools legacy WebSocket executor package.	N/A	More Deta
CVE-2026-118260	Echo is a Go web framework. From 4.0.0 until 4.16.1, Echo v4's opt-in BodyDump middleware reads complete request bodies into memory before handlers run and retains complete response bodies for the dump callback without capture limits. An unauthenticated client that can reach a route using BodyDump can submit large bodies or influence large responses, causing repeated or concurrent allocations that exhaust process memory. BodyDump is not enabled by default, and external request limits may reduce request-side exposure but do not bound response capture. This issue is fixed in 4.16.1.	N/A	More Deta
CVE-2026-118255	Highcharts JS is a JavaScript charting library based on SVG. From 2.0.0 until 3.2.0, Highcharts Grid applies credits.href to the credits link without validating the URL scheme. An attacker who controls Grid configuration can provide a javascript URL, and activating the credits link runs script in the origin of the hosting page with access to that application's data and session state.This issue is fixed in Grid Pro 3.2.0.	N/A	More Deta
CVE-2026-116266	MIME::Head versions from 5.518 before 5.521 for Perl decode a partly encoded multipart boundary without flagging the parse as ambiguous. The multipart_boundary() method decodes RFC 2047 encoded words anywhere in the boundary, but the ambiguity check only fires when the whole value is one encoded word. A boundary such as abc=?us-ascii?Q?def?= is used as abcdef, and ambiguous_content() returns false. Encoded words are not allowed in parameters, so other mail readers split the message on the literal value. A remote sender can hide an attachment from a filter that relies on ambiguous_content() while the recipient's mail client shows it.	N/A	More Deta
CVE-2026-117500	HTTP::Body versions before 1.24_01 for Perl allow CPU exhaustion via regex backtracking on the filename of a multipart upload. For every file part, the multipart parser finds the suffix of the uploaded filename by matching the default $basename_regexp, qr/[^.]+(\.[^\\\/]+)$/, against the whole basename. A basename made of many dots and ending in a backslash makes the regex backtrack in time quadratic in its length. A remote attacker can exhaust CPU with one request, as a basename of about 32 KB takes several seconds to match and every file part is matched separately.	N/A	More Deta
CVE-2026-	MIME::Parser versions before 5.521 for Perl allow memory exhaustion via indented error messages from a truncated, deeply nested message. Each stored parser diagnostic is indented by three spaces per nesting level. When a message nested N levels deep ends without its closing boundaries,	N/A	More Deta

116267	every level logs an error at its own depth, so the stored diagnostics grow with the square of N. The defaults place no limit on nesting depth.		
CVE-2026-116268	MIME::Field::ParamVal versions before 5.521 for Perl allow CPU exhaustion via unclosed comments in header parameters. The comment pattern used to parse Content-Type and Content-Disposition parameters scans from each "(" to the next ")". In a field with no ")", every "(" scans to the end of the header and fails, so parsing takes time quadratic in the header length. The field is parsed again on each attribute lookup, several times per MIME entity. A 40 KB header takes about 7 seconds to parse once.	N/A	More Deta
CVE-2026-116269	MIME::Field::ParamVal versions before 5.521 for Perl turn an RFC 2231 filename with a hyphenated language tag into an empty recommended filename. A parameter such as filename*=utf-8'en-US'payload.exe is converted to an encoded word with the language tag appended to the charset. The decoder strips the language suffix only when it is a single word, so it cannot resolve the charset UTF-8*EN-US and returns an empty string. The recommended_filename() method returns that empty string rather than falling back to the name parameter. Other mail readers return payload.exe. A remote sender can get an attachment past a policy that checks file extensions on the recommended filename.	N/A	More Deta
CVE-2026-116270	MIME::Words versions before 5.521 for Perl allow memory exhaustion via repeated "=?" sequences in decode_mimewords. For each "=?" that does not start a complete encoded word, decode_mimewords appends an error message containing the whole input string to $@. A boundary of 8,000 "=?" pairs (16,000 bytes) adds 8,000 copies of itself to $@, about 128 MB. From version 5.518, MIME::Parser decodes every multipart boundary this way, so a remote sender can exhaust the memory of the parsing process with one Content-Type header.	N/A	More Deta
CVE-2026-116271	MIME::Parser::FileUnder versions before 5.521 for Perl reuse a pre-created output directory and follow symlinks in it, letting local users redirect attachment writes. Each message is written to a directory named msg-<time>-<pid>-<n> under the output base, and an existing directory of that name is used as is. A file name counts as unused when nothing exists at that path, which holds for a dangling symlink, and the body file is then opened in a way that follows the link. When the output base is writable by other users, as with output_under("/tmp"), a local user can pre-create the directory with a symlink named like an attachment. The parser then writes the attachment to the link target with the privileges of the parsing process.	N/A	More Deta
CVE-2026-116272	MIME::Field::ParamVal versions before 5.521 for Perl do not flag a duplicate boundary parameter whose name contains a nested comment. A parameter written boundary((c))="A" or boundary(\))="A" is stored under that literal name rather than as boundary. A second boundary parameter is then not reported as a duplicate, and MIME::Parser splits the message on it. Readers that skip comments as RFC 5322 allows take the first boundary instead. A remote sender can hide an attachment from a filter that relies on ambiguous_content() while the recipient's mail client shows it.	N/A	More Deta
CVE-2026-116273	MIME::Parser versions before 5.521 for Perl set no limit on the number of message parts by default, allowing memory exhaustion. The max_parts option defaulted to -1, which disables the limit, so a parser created with default settings builds an entity for every part however many a message has. Version 5.521 sets max_parts to 1000 and max_depth to 64 by default. Setting either to -1 still removes the limit.	N/A	More Deta
CVE-2026-116285	HTTP::Body versions before 1.23_01 for Perl allow CPU exhaustion via quadratic regex backtracking when parsing chunked request bodies. In chunked mode, used when no content length is given, add() matches each chunk-size line with `/^([\da-fA-F]+).*\x0D\x0A/`. On a line of hex digits whose first LF has no CR before it, the digits and `.*` backtrack against each other, so a single add() takes time quadratic in the line's length. Nothing limits how long the line can be. A remote attacker can exhaust CPU in applications that pass chunked request bodies to HTTP::Body.	N/A	More Deta
CVE-2026-116531	HTTP::Body versions before 1.23_01 for Perl lose track of chunk boundaries in chunked request bodies when a read ends inside a chunk. In chunked mode, used when no content length is given, add() treats a chunk as complete once the buffer is as long as the chunk's declared size, but the buffer still holds the chunk-size line. When a read ends in the last bytes of a chunk, add() takes the chunk short and parses the leftover data as the next chunk-size line. A remote attacker can make a chunked body never complete, hanging a server that reads until the body is done, and may make it complete early, leaving the remaining bytes to be read as the next request.	N/A	More Deta
CVE-2026-116794	russh is a Rust SSH client and server library that includes an SSH agent protocol implementation. From 0.50.0-beta.12 until 0.65.0, the agent server's Connection::try_sign path in russh/src/keys/agent/server.rs recognizes SSH_AGENT_CONSTRAIN_CONFIRM but returns a hard-coded successful result instead of calling Agent::confirm. In applications that override Agent::confirm to require user approval or another policy check, a process that can reach the agent socket, including the remote side of a forwarded agent, can use a key added through ssh-add -c without that check and can authenticate or sign data as the user while the key remains loaded. The separate Agent::confirm_request hook still runs for every signing request, so checks implemented there remain effective, and implementations that retain the default always-successful Agent::confirm do not lose an approval check through this regression. This issue is fixed in version 0.65.0.	N/A	More Deta
CVE-2026-117812	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-116796	Highcharts JS is a JavaScript charting library based on SVG. From 10.3.2 until 11.4.9, 12.6.2, and 13.1.1, Highcharts accepts an SVG anchor xlink:href attribute without applying the allowed-scheme check used for href and src. An attacker who controls a chart text option can preserve a javascript URL in serialized chart output. When exported or server-rendered SVG is parsed again and a user activates the link, script runs in the origin of that document. This issue is fixed in 11.4.9, 12.6.2 and 13.1.1.	N/A	More Deta
CVE-2026-116797	Highcharts JS is a JavaScript charting library based on SVG. From 2.0.0 until 3.2.0, Highcharts Grid Pro input renderers copy the cells.renderer.attributes and cells.editMode.renderer.attributes maps to input or select elements with raw setAttribute calls. An attacker who controls column configuration can add event-handler attributes to every rendered row or to the control created when a cell enters edit mode. Script then runs in the hosting page origin when a user hovers over or focuses an input or begins editing. This issue is fixed in Grid Pro 3.2.0.	N/A	More Deta
CVE-2026-117501	HTTP::Body versions before 1.24_01 for Perl allow memory exhaustion via unbounded buffering of chunked request bodies. In chunked mode, used when no content length is given, add() holds each chunk in memory until all of it has arrived. A line that is not a chunk-size line, a size line without CRLF, or a size too large to fit an integer leaves the parser waiting forever, and every later add() grows the buffer. A remote attacker can exhaust memory in applications that pass chunked request bodies to HTTP::Body.	N/A	More Deta
CVE-2026-118254	Highcharts JS is a JavaScript charting library based on SVG. From 2.0.0 until 3.2.0, Highcharts Grid writes pagination language strings into the DOM as markup instead of text. An attacker who controls the Grid language configuration can provide elements with event handlers, which execute in the hosting page origin when pagination controls render. Exploitation requires pagination to be enabled but does not require additional user interaction. This issue is fixed in 3.2.0.	N/A	More Deta
CVE-2026-118242	Highcharts JS is a JavaScript charting library based on SVG. From 2.3.0 until 3.2.0, Highcharts Grid creates SVG path elements from rendering.icons object definitions and previously copied every child key with setAttribute. An attacker who controls Grid configuration can supply event-handler attribute names in an icon definition. Because custom icons override built-ins, the attacker can replace default sort or pagination icons, and script runs in the hosting page origin when a user hovers over or activates the affected icon. This issue is fixed in 3.2.0.	N/A	More Deta
CVE-2026-118243	Highcharts JS is a JavaScript charting library based on SVG. From 1.0.0 until 4.2.2, Highcharts Dashboards stores DataCursor listener and state maps in plain objects keyed by DataTable ID. A __proto__ table ID supplied through dataPool connector configuration resolves to Object.prototype, and sync registration creates an enumerable property there whose suffix can be influenced through the sync group option. The property is visible on every object, and lasting sync states can throw and stop features such as extremes synchronization. Exploitation requires untrusted dashboard	N/A	More Deta

	configuration and an enabled component sync, but no user interaction beyond loading the board. This issue is fixed in 4.2.2.		
CVE-2026-118244	Highcharts JS is a JavaScript charting library based on SVG. From 12.0.0 until 12.6.1 and 13.1.0, Highcharts falls back to assigning raw markup to innerHTML when DOMParser cannot return a document, before its allow-list is applied. In Chromium, the Trusted Types callback can throw while a beforeprint handler runs, so a page that redraws a chart during beforeprint can insert untrusted HTML text options into the hosting document. Event handlers in that markup then run in the page origin when printing begins. The issue affects HTML-rendered titles, labels, data labels, responsive text, and the Stock, Maps, and Gantt products shipped in the same package. This issue is fixed in 12.6.1 and 13.1.0.	N/A	More Deta
CVE-2026-118245	Highcharts JS is a JavaScript charting library based on SVG. From 1.0.0 until 4.2.2, Highcharts Dashboards uses chartConstructor as an unchecked property lookup in the Highcharts namespace and invokes the selected member with the component container and chartOptions. An attacker who controls dashboard configuration can select a public utility function instead of a supported chart constructor, causing attacker-controlled options to be copied to the container as properties or attributes. Markup and event handlers can then execute in the hosting page origin when the board renders. No user interaction beyond rendering the board is required. This issue is fixed in 4.2.2.	N/A	More Deta
CVE-2026-118246	Highcharts JS is a JavaScript charting library based on SVG. From 10.0.0 until 11.4.9, 12.6.1, and 13.1.0, Highcharts applies breadcrumbs.style as SVG attributes rather than CSS and does not filter the attribute names. An attacker who controls chart configuration can provide event-handler keys through drilldown.breadcrumbs, navigation.breadcrumbs, or hierarchical series breadcrumb options. The keys become active handlers on the breadcrumb button and execute in the hosting page origin after the user navigates to a level and hovers over or activates the button. Styled-mode charts do not apply this option and are not affected. This issue is fixed in 11.4.9, 12.6.1 and 13.1.0.	N/A	More Deta
CVE-2026-118247	Highcharts JS is a JavaScript charting library based on SVG. From 1.0.0 until Dashboards 4.2.2, and from 2.0.0 until Grid Pro 3.2.0, Highcharts DataTable single-cell writers use an untrusted column ID as a key without rejecting __proto__ or constructor. DataTable.setCell, including Dashboards connector write-back and Grid Pro editing paths, can therefore write integer-indexed values onto Object.prototype or the Object constructor. In Dashboards releases with column aliases, a literal __proto__ ID is redirected by the alias map, while an alias targeting __proto__ reaches the unsafe write; later releases without aliases accept the unsafe ID directly. Those inherited values affect array and object reads and for-in enumeration throughout the page, which can alter application control flow or disrupt rendering. Exploitation requires control of the table or component column ID and a cell, point, or API write. This issue is fixed in Dashboards 4.2.2 and Grid Pro 3.2.0.	N/A	More Deta
CVE-2026-118248	Highcharts JS is a JavaScript charting library based on SVG. From 1.0.0 until 4.2.2, Highcharts Dashboards edit mode walks editableOptions propertyPath segments without rejecting prototype-related keys. An attacker who controls editableOptions can provide a path through __proto__ or constructor, and a user's edit writes the configured value onto Object.prototype. The property then becomes visible to JavaScript throughout the page, with consequences determined by the consuming application. This issue is fixed in 4.2.2.	N/A	More Deta
CVE-2026-118249	Highcharts JS is a JavaScript charting library based on SVG. From 13.0.0 until 13.1.0, Highcharts builds series data columns by using point option keys directly as column IDs. Own enumerable __proto__ and constructor keys from parsed point objects can therefore direct integer-indexed writes to Object.prototype or the Object constructor. The inherited values affect reads and for-in enumeration across the page and can disrupt rendering or alter consuming application behavior without user interaction beyond rendering the chart. This issue is fixed in 13.1.0.	N/A	More Deta
CVE-2026-118250	Highcharts JS is a JavaScript charting library based on SVG. From 6.1.0 until 11.4.9, 12.6.1, and 3.1.0, Highcharts follows dot-separated series.keys paths without filtering each segment. An attacker who controls series.keys and matching point data can use a path through __proto__ to assign arbitrary named properties to Object.prototype. Those properties are visible to all JavaScript in the page, and no user interaction is required beyond rendering the chart. This issue is fixed in 11.4.9, 12.6.1, and 3.1.0.	N/A	More Deta
CVE-2026-117811	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-118251	Highcharts JS is a JavaScript charting library based on SVG. Prior to 11.4.9, 12.6.1, and 13.1.0, Highcharts assigns credits.href to the window location when the credits label is clicked without checking the URL against the allowed-scheme list. An attacker who controls chart configuration can provide a javascript URL and run script in the origin of the hosting page when a user clicks the credits label. Highcharts Stock, Maps, and Gantt are included because they ship from the same package. This issue is fixed in 11.4.9, 12.6.1 and 13.1.0.	N/A	More Deta
CVE-2026-118252	Highcharts JS is a JavaScript charting library based on SVG. From 1.0.0 until 4.2.3, Highcharts Dashboards edit-mode sidebar parses component language strings as HTML rather than inserting them as text. An attacker who controls the Dashboards language configuration can provide markup containing event handlers, which execute in the hosting page origin when a user opens the edit-mode sidebar and the affected labels render. This issue is fixed in 4.2.3.	N/A	More Deta
CVE-2026-118253	Highcharts JS is a JavaScript charting library based on SVG. From 1.0.0 until 4.2.3, Highcharts Dashboards edit mode parses fullscreen language labels as HTML rather than inserting them as text. An attacker who controls Dashboards language options can supply markup with event handlers, which execute in the hosting page origin when the fullscreen control is rendered. The label is reachable only when edit mode is enabled and viewFullscreen is present in the context-menu items. This issue is fixed in 4.2.3.	N/A	More Deta
CVE-2026-117836	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117837	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-118669	OAuthLib is an implementation of the OAuth request-signing logic for Python 3.6+. Prior to 4.0.0, the client_credentials and Resource Owner Password Credentials token grant handlers can authenticate request.client as one confidential client while retaining an attacker-supplied request.client_id for validate_grant_type and validate_scopes. A lower-privilege authenticated client can therefore cause grant and scope authorization to use another client's identity when an application validator relies on the documented client_id argument, potentially issuing tokens with unauthorized grants or scopes. Validators that authorize exclusively from request.client may not be affected. This issue is fixed in version 4.0.0.	N/A	More Deta
CVE-2026-116776	USB Test is a lightweight Windows CLI utility for verifying sector integrity and detecting overreported capacity on USB flash drives. Prior to version 1.1.5, getSectorSize() in USB Test/src/driveinfo.cpp trusts DISK_GEOMETRY.BytesPerSector returned by IOCTL_DISK_GET_DRIVE_GEOMETRY without checking whether the call succeeded or enforcing size bounds. USB Test/src/drivetest.cpp uses the value for division and to size a heap buffer before memcpy(buffer.data(), &sector, 8), so a physically connected malicious USB storage device can report a value below eight bytes and cause repeated out-of-bounds writes, or report zero and cause a divide-by-zero denial of service when a user starts a drive test. The heap corruption can crash the elevated application and may permit arbitrary code execution. This issue is fixed in version 1.1.5.	N/A	More Deta
	In the Linux kernel, the following vulnerability has been resolved: sched_ext: Fix stall when a task enqueued with SCX_ENQ_LAST lands back on its CPU's local DSQ With SCX_OPS_ENQ_LAST, the last runnable task on a CPU is passed to ops.enqueue() instead of being kept running. Exiting tasks without SCX_OPS_ENQ_EXITING, migration disabled tasks without SCX_OPS_ENQ_MIGRATION_DISABLED and tasks on an offline rq skip		

CVE-2026-99105	ops.enqueue() and go straight to the local DSQ. This happens in put_prev_task_scx() after the pick has settled on idle, so nothing reschedules the CPU, which idles with the task queued until an unrelated wakeup lands on it or the watchdog fires. scx_mitosis, which sets SCX_OPS_ENQ_LAST without SCX_OPS_ENQ_EXITING, hit this during mass cgroup teardown: exiting tasks stuck in exit_mmap() for over 40 seconds. A task put on the local DSQ runs, as anywhere else. If the SCX_ENQ_LAST enqueue left the task on this CPU's local DSQ, set need_resched on the task being switched in, as proxy_resched_idle() does. resched_curr() would flag the task being put instead, and __schedule() clears that right after the pick.	N/A	More Deta
CVE-2026-99155	In the Linux kernel, the following vulnerability has been resolved: scsi: xen/scsifront: Check for a NULL shadow entry on a backend response scsifront_do_response() validates the rqid in a backend response against VSCSIIF_MAX_REQS before using it to index info->shadow[], but then dereferences the entry to test ->inflight without checking that the slot is populated. Shadow slots are NULL before a command is submitted (the host private area is zeroed at allocation) and are reset to NULL in _scsifront_put_rqid() once a request completes, so an in-range rqid that does not correspond to an outstanding request makes the frontend dereference a NULL pointer. A malicious or buggy backend can thus crash the guest by returning a response whose rqid is in range but not in flight -- for example a spurious response before any command has been issued, or a duplicate of one already completed. The ring has only VSCSIIF_MAX_REQS (16) slots, so before the first command every in-range rqid selects a NULL slot. Reject a response whose shadow slot is not populated.	N/A	More Deta
CVE-2026-99104	In the Linux kernel, the following vulnerability has been resolved: sched_ext: Fix the bypass dispatch claim for schedulers bypassed by an ancestor scx_bypass() claims bypass dispatch when the scheduler's depth goes from zero to one and releases it when the depth returns to zero, but propagates only the depth to the descendants, not the claim. A descendant that starts bypassing with its ancestor never claims, and one whose own bypass ends under the ancestor's keeps its claim, as its depth does not return to zero. A sub-scheduler enable whose bypass ends under a PM suspend thus leaks its claim: the parent keeps hosting bypass dispatch and the sub-scheduler's next bypass trips the WARN_ON_ONCE() on the claim. A sub-scheduler disable that starts under a PM suspend has no claim, so once the resume lifts the root's bypass its tasks sit on the parent's bypass DSQs with nobody consuming them. Claim for every descendant whose depth goes from zero to one in the propagation and release every scheduler in the subtree whose depth returned to zero once the tasks have moved out of the bypass DSQs. A parent that is bypassing itself when a descendant claims consumes only its own bypass DSQs, empty until it leaves bypass and becomes the host.	N/A	More Deta
CVE-2026-99157	In the Linux kernel, the following vulnerability has been resolved: scsi: bsg: Pass reply_len to bsg_setup_queue() to fit UFS ARPMB replies bsg-lib allocates a 96-byte (SCSI_SENSE_BUFFERSIZE) reply buffer per job, but struct ufs_rpmb_reply is 104 bytes: a 40-byte struct ufs_bsg_reply followed by a 64-byte EHS. When an Advanced RPMB command returns an EHS, ufshcd_advanced_rpmb_req_handler() copies it right after the 40-byte header and writes 8 bytes past the end of the buffer. Let each BSG transport pass its reply buffer size to bsg_setup_queue() and have ufs_bsg request sizeof(struct ufs_rpmb_reply), so the full reply reaches user space. Other transports keep SCSI_SENSE_BUFFERSIZE.	N/A	More Deta
CVE-2026-99158	In the Linux kernel, the following vulnerability has been resolved: ring-buffer: Fix false warning in ring_buffer_map_get_reader() The mmap reader can warn when it catches up with a writer that is still committing events. rb_get_reader_page() returns NULL in this case, but ring_buffer_map_get_reader() treats that result as an error. The initial rb_per_cpu_empty() check filters out an empty buffer, but it does not guarantee that the next reader page has committed data. Writers do not take reader_lock and can advance commit_page before publishing the committed length on the new page. rb_get_reader_page() can swap to that page, catch up with the writer and return NULL. Handle NULL through the existing no-data exit without warning. Remove the caller's reader_page == commit_page check as well, since the reader-page helper already handles that case. The existing metadata update and return path remain in place.	N/A	More Deta
CVE-2026-99159	In the Linux kernel, the following vulnerability has been resolved: ring-buffer: Fix the sub-buffer array base in rb_meta_subbuf_idx() On a persistent ring buffer, rb_meta_subbuf_idx() can return an index one sub-buffer too high. rb_setup_ids_meta_page() then fills subbuf_ids[] shifted by one and leaves subbuf_ids[0] NULL, which __rb_map_vma() dereferences when userspace maps trace_pipe_raw. rb_update_meta_reader() writes two such indices into meta->buffers[], which rb_cpu_meta_valid() would reject on the next boot, discarding the previous boot's trace. A CPU's sub-buffer array starts after its meta header and the nr_subbufs integers that follow, aligned up to a sub-buffer. rb_meta_subbuf_idx() inverts that calculation but skips only the integers, not the header, so its base is one sub-buffer low whenever the omitted header size crosses the alignment boundary. Invert the calculation with rb_subbufs_from_meta() rather than repeating it. rb_range_buffer() maps an index back to an address through the same helper, so the two directions can no longer disagree.	N/A	More Deta
CVE-2026-99160	In the Linux kernel, the following vulnerability has been resolved: ring-buffer: Do not show buffer_meta for CPUs without a buffer The per_cpu/cpuN/buffer_meta files are created for every possible CPU, but buffer->buffers[cpu] is only allocated once that CPU comes online. Reading the file of a CPU that never came online dereferences a NULL cpu_buffer in rbm_start(). Fail the open with -ENODEV when the CPU has no buffer, as the other per CPU ring buffer interfaces do.	N/A	More Deta
CVE-2026-99161	In the Linux kernel, the following vulnerability has been resolved: i2c: viai2c-wmt: Fix clock leak in wmt_i2c_probe() In wmt_i2c_probe(), i2c->clk is acquired using of_clk_get(). If any subsequent operation fails or when the module is unloaded, the clock reference count is never decremented via clk_put(), leading to a resource leak. Switch to devm_clk_get() so that the clock is automatically managed and released.	N/A	More Deta
CVE-2026-99162	In the Linux kernel, the following vulnerability has been resolved: gpio: shared: fix use-after-free bug when adding shared proxies The GPIO lookup table can stay alive for longer than the kobject whose name string's address we're assigning to lookup->dev_id. Fix a potential UAF by duplicating the string.	N/A	More Deta
CVE-2026-99103	In the Linux kernel, the following vulnerability has been resolved: workqueue: Fix unbound pool lifetime for pending pwqs KASAN reports a use-after-free of an unbound worker_pool in node_activate_pending_pwq(): BUG: KASAN: slab-use-after-free in _raw_spin_trylock+0x6d/0x120 Read of size 4 at addr ffff8880089ce000 by task kworker/u22:0/318 CPU: 1 UID: 0 PID: 318 Comm: kworker/u22:0 Not tainted 7.2.0 #1 PREEMPT(lazy) Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.15.0-1 04/01/2014 Workqueue: 0x0 (flush-8:0) Call Trace: <TASK> dump_stack_lvl+0x53/0x70 print_report+0xce/0x610 kasan_report+0xce/0x100 _raw_spin_trylock+0x6d/0x120 pwq_dec_nr_in_flight+0x4b4/0xcb0 process_one_work+0x921/0x11a0 worker_thread+0x4d0/0xd20 kthread+0x2de/0x3c0 ret_from_fork+0x3aa/0x620 ret_from_fork_asm+0x1a/0x30 </TASK> Allocated by task 311: alloc_pwq+0x439/0xca0 apply_wqattrs_prepare+0x75e/0xd10 apply_workqueue_attrs_locked+0x44/0xa0 wq_nice_store+0x350/0x450 Freed by task 0: kfree+0x127/0x3b0 rcu_core+0x523/0x1780 handle_softirqs+0x1b3/0x610 Last potentially related work creation: put_unbound_pool+0x3f3/0x7d0 pwq_release_workfn+0x494/0x8e0 kthread_worker_fn+0x1ff/0x790 Canceling the last inactive work skips pwq_dec_nr_active(), so an empty pwq can remain on pending_pwqs when its refcnt reaches zero. pwq_release_workfn() currently puts the pool before removing that pwq. If this drops the last pool reference, the pool can be RCU-freed while the pwq remains reachable, and node_activate_pending_pwq() may trylock the freed pool->lock. Remove the pwq from pending_pwqs before putting the pool.	N/A	More Deta
CVE-2026-99102	In the Linux kernel, the following vulnerability has been resolved: ntfs: take invalidate_lock in ntfs_setattr_size() ntfs_setattr_size() updates i_size and resizes the on-disk attribute without holding mapping->invalidate_lock. Page faults take the lock shared, so a fault racing the resize can resolve a VCN against the transient runlist state of ntfs_non_resident_attr_expand() and fail with a spurious SIGBUS, and can interleave with the size-change epilogue (truncate_pagecache(), i_size_write(), pagecache_isize_extended()). Take invalidate_lock exclusively around the whole resize after inode_dio_wait(), matching the fallocate path and other filesystems such as xfs, which wraps truncate in its mmaplock (= invalidate_lock).	N/A	More Deta
	In the Linux kernel, the following vulnerability has been resolved: sctp: revalidate output stream after association connect wait When message interleaving is enabled, the first send waits for association establishment before building its data chunks. The wait drops the socket lock, and handshake processing can reduce the output stream count to the peer-advertised inbound stream count. sctp_stream_init() then frees the extension of every removed stream. The sender resumes with the stream that it checked before the wait. If the peer removed that stream, sctp_outq_tail() later dereferences its NULL extension. Fatal-oops policies then panic the host. KASAN: null-ptr-deref in range [0x38-0x3f] RIP:		

CVE-2026-99165	sctp_outq_tail+0x49e/0xaa0 Call Trace: sctp_primitive_SEND sctp_sendmsg_to_asoc sctp_sendmsg A range check alone is insufficient. Stream reconfiguration can grow the output count again while the lock is released without recreating extensions freed by the earlier shrink. The stream can then be in range while its extension remains NULL. The send-buffer wait has the same issue. Factor the range and extension checks into a helper and repeat both after each send-path wait that drops the socket lock. Once the lock is reacquired, the validation remains stable through data creation and queueing. If validation fails after the connect wait, the auto-created association is already established. Return ESRCH so the existing caller path keeps it under state-machine ownership instead of freeing it directly, which would leave protocol, counter and socket state inconsistent.	N/A	More Deta
CVE-2026-99166	In the Linux kernel, the following vulnerability has been resolved: net: rds: fix uninitialized trans dereference in CM event handler rds_rdma_cm_event_handler_cmn() assigns trans only when the RDMA device is an InfiniBand CA (RDMA_NODE_IB_CA). On any other device type, e.g. an iWARP RNIC such as siw, trans stays uninitialized, but the event switch dereferences it: unconditionally in the RDMA_CM_EVENT_CONNECT_REQUEST case via trans->cm_handle_connect(), and (with a connection context) in the ROUTE_RESOLVED and ESTABLISHED cases. An RDS listener on an iWARP device therefore crashes the kernel as soon as a connect request arrives: with CONFIG_INIT_STACK_ALL_ZERO the wild load becomes a NULL dereference at offset 0xa0 (&trans->cm_handle_connect) in the iw_cm_wq workqueue. GCC masks the bug in default builds by folding the uninitialized load into &rds_ib_transport; Clang-built kernels take the real uninitialized path and oops. The active side can land on a non-IB device too: the id that rds_ib_conn_path_connect() creates is not restricted to a node type, so rdma_resolve_addr() binds it to whichever device serves the local address, and an iWARP RNIC on the same netdev qualifies. The crash there is different: resolving a route on an iWARP id never fills in cm_id->route.path_rec, and the ROUTE_RESOLVED case writes path_rec[0].sl before it calls into the transport. The iWARP transport was dropped long ago and IB is the only transport left, so make that explicit: initialize trans to &rds_ib_transport at declaration, drop the conditional assignment, reject a connect request that arrives on a non-IB device, and drop a connection whose address resolved to one instead of resolving a route on it. The rejection is limited to RDMA_CM_EVENT_CONNECT_REQUEST on purpose: a non-zero return from the handler makes rdma_cm destroy the id the event was delivered on, which is right for the request's freshly created id but would free a connection id that RDS still owns for any other event. On the active side the id stays ic->i_cm_id and the connection's shutdown destroys it, so that case returns 0. [achender: reject only on RDMA_CM_EVENT_CONNECT_REQUEST instead of bailing out for every event on a non-IB device, so that rdma_cm does not destroy connection ids RDS still tracks; drop a connection whose address resolved to a non-IB device before a route is resolved on it; changelog adjusted]	N/A	More Deta
CVE-2026-99101	In the Linux kernel, the following vulnerability has been resolved: ntfs: move attribute payload before shrinking its record ntfs_new_attr_flags() resizes the non-resident attribute record before moving its name and mapping pairs to their shorter-header offsets when compression or sparse state is cleared. Shrinking the record first moves the following attribute over the tail of the old record. The subsequent memmove() therefore copies bytes from that following attribute instead of the old mapping pairs. Re-enabling compression on an empty file persists those bytes as a malformed mapping pairs array, which ntfsck reports as a missing or invalid run length. Move the payload before shrinking the record, while retaining the existing resize-before-move ordering when growing it.	N/A	More Deta
CVE-2026-99168	In the Linux kernel, the following vulnerability has been resolved: mshv_vtl: Check per-CPU register page before mmap Register-page setup is optional for each CPU. If allocation or registration fails, mshv_vtl_configure_reg_page() warns and leaves that CPU's reg_page NULL, but initial context setup continues successfully. Meanwhile, successful setup on another CPU sets the global mshv_has_reg_page flag. mshv_vtl_fault() checks this global flag before selecting the requested CPU's register page. With mixed setup results across online CPUs, the check passes even for a CPU with no register page, reaching get_page(NULL) when userspace faults in that mapping. Check the selected per-CPU register page before taking its reference and return VM_FAULT_SIGBUS if it is absent.	N/A	More Deta
CVE-2026-99169	In the Linux kernel, the following vulnerability has been resolved: futex: Fix mm reuse handling for FUT_OFF_MMSHARED A FUT_OFF_MMSHARED futex is a shared futex that refers to an MM. It is possible for a process to wait on a shared futex with a different MM because a FUT_OFF_INODE waiter can be requeued onto a FUT_OFF_MMSHARED futex by another process. This can cause FUT_OFF_MMSHARED waiters on a freed MM to consume wakeups intended for a newly allocated MM at the same address. Fix it by keying FUT_OFF_MMSHARED using a unique 64-bit per-MM ID. Leave private futexes as before to avoid influencing the performance of the hotpath. (Multi-threaded processes typically implicitly use FUT_OFF_MMSHARED by setting clear_child_tid such that it points into anonymous memory, which causes mm_release() in a multi-threaded mm to perform FUTEX_WAKE.)	N/A	More Deta
CVE-2026-87880	Sensitive information disclosure due to missing SSL certificate verification affecting one component. The following products are affected: Acronis Cyber Protect 17 (Linux, Windows) before build 42587.	N/A	More Deta
CVE-2026-99171	In the Linux kernel, the following vulnerability has been resolved: ntfs3: free the sbi after a grace period If the "nocase" mount option ntfs3 uses custom hash and dentry compare functions. Both access ntfs3 superblock private information in rcu pathwalk. ntfs_put_super() and ntfs3_kill_sb() drop the info without any rcu delay. A lookup that's still inside the filesystem when the last reference to the mount is dropped causes a UAF. With a pathwalk held up in ntfs_d_hash() while the last reference to the mount goes away: BUG: KASAN: slab-use-after-free in ntfs_nls_to_utf16+0x752/0x940 Read of size 8 at addr ff1100010453c850 by task walker/99 Call Trace: <TASK> ntfs_nls_to_utf16+0x752/0x940 ntfs_d_hash+0x22b/0x500 link_path_walk+0x11ad/0x1d30 path_lookupat+0x63/0xb00 filename_lookup+0x1f1/0x5b0 vfs_statx+0xd7/0x3b0 [...] Allocated by task 95: __kmalloc_cache_noprof+0x249/0x560 ntfs_init_fs_context+0x2db/0x5a0 alloc_fs_context+0x52e/0xc70 [...] Freed by task 98: kfree+0x1db/0x5b0 deactivate_locked_super+0x9c/0xf0 cleanup_mnt+0x9f/0x130 task_work_run+0x131/0x250 The bug is currently masked by the grace period in namespace_unlock() for umount(2). Keep the necessary information until the filesystem private info is freed and free it with an rcu delay. ntfs3_free_sbi() now runs from an rcu callback and drops the upcase table via ntfs_put_shared(). So switch s_shared_lock over to spin_lock_bh(). Otherwise the callback can deadlock against a task holding the lock on the same cpu.	N/A	More Deta
CVE-2026-99172	In the Linux kernel, the following vulnerability has been resolved: ipc: drop the mqueue mount with kern_unmount() on setup failure mq_init_ns() creates the mqueue mount with fc_mount_longterm(), so its ->mnt_ns is MNT_NS_INTERNAL. When setting up the mqueue or ipc sysctls or msg_init_ns() fails afterwards, create_ipc_ns() drops it with a plain mntput(). With ->mnt_ns set that takes the fast path of mntput_no_expire(). The count drops to zero and nothing ever kills the mount, so the mount and the mqueue superblock are leaked. Commit dc55e35f9e81 ("ipc: Store mqueue sysctls in the ipc namespace") added the first failure path after mq_init_ns() and never dropped the mount. Commit 7229d74e5e8c ("ipc: create_ipc_ns: drop mqueue mount on sysctl setup failure") tried to fix that with a mntput() but that doesn't help for a long-term mount. Use kern_unmount(). free_ipc() open-codes the same thing for a namespace that made it.	N/A	More Deta
CVE-2026-87879	Sensitive information disclosure due to improper token validation. The following products are affected: Acronis Cyber Protect 17 (Linux, Windows) before build 42587.	N/A	More Deta
CVE-2026-99174	In the Linux kernel, the following vulnerability has been resolved: ext4: free the sbi after a grace period ext4_get_link() follows a symlink that keeps its target in a data block in rcu pathwalk mode with ext4_getblk(EXT4_GET_BLOCKS_CACHED_NOWAIT). That reads s_mount_state in the ASSERT() of ext4_getblk() and again in ext4_es_lookup_extent(), and the lookup bumps the extent status hit or miss counter, all through sb->s_fs_info. ext4_put_super() destroys those counters, clears sb->s_fs_info and frees the sbi without waiting for a grace period. A pathwalk that is still in ext4_get_link() when the last reference to the mount goes away then dereferences a NULL s_fs_info, the freed sbi or the destroyed percpu counters. With a pathwalk held up in ext4_get_link() while the last reference goes away: KASAN: null-ptr-deref in range [0x00000000000000a8-0x00000000000000af] RIP: 0010:ext4_getblk+0xf0/0x640 Call Trace: <TASK> ext4_get_link+0x26c/0x410 pick_link+0xf96/0x1780 step_into_slowpath+0x9b8/0x1250 path_lookupat+0x484/0xb00 filename_lookup+0x1f1/0x5b0 vfs_statx+0xd7/0x3b0 vfs_fstatat+0x4d/0x90	N/A	More Deta

	__do_sys_newfstatat+0xa0/0x100 do_syscall_64+0x10e/0x5e0 entry_SYSCALL_64_after_hwframe+0x77/0x7f So far that has been hard to hit. umount(2) waits for a grace period in namespace_unlock() before it drops the mount, so only a mount whose last reference goes away elsewhere, like the close of a file or a chdir out of a lazily unmounted directory, can race a walker. Keep sb->s_fs_info and free the sbi together with the extent status counters after a grace period. Split the counters out of ext4_es_unregister_shrinker() for that. The shrinker still gets wasted in ext4_put_super(), the counters go with the sbi.		
CVE-2026-99175	In the Linux kernel, the following vulnerability has been resolved: fsnotify: prevent mark additions during connector teardown fsnotify_destroy_marks() keeps a reference to its current mark while it drops conn->lock to destroy the mark. This stabilizes the forward-walk cursor, but does not prevent a new mark from being inserted before it. For example, an inotify watch re-added after IN_IGNORED sorts before the old, detached mark for the same group. The walk can miss the replacement and then detach the entire connector from the object. The replacement is still on its group's marks_list and, for inotify, in the watch IDR. The group mutex no longer protects the connector's object from disappearing. An unprivileged fdinfo read racing the final detach can consequently call igrab(NULL): BUG: KASAN: null-ptr-deref in igrab+0x24/0x100 Write of size 4 at addr 0000000000000148 Call Trace: igrab+0x24/0x100 inotify_show_fdinfo+0x1dc/0x5e0 seq_show+0x397/0x690 Set a DESTROYING flag under conn->lock before starting the walk, and reject new marks on that connector with -ENOENT. The existing add-mark error paths undo the temporary group-list entry and the backend's watch allocation. Do not wait for teardown while holding the group mutex, which the destroyer needs. Once the old connector is detached, an add can install a fresh connector as before. This closes the insertion race for all object types using the common connector teardown, without changing the mark reference or SRCU lifetime rules.	N/A	More Deta
CVE-2026-99176	In the Linux kernel, the following vulnerability has been resolved: KVM: nVMX: Reset MMU back to the root MMU if loading L2 state fails for !VM-Entry Reset the vCPU's MMU pointer back to the root MMU if loading L2 state fails in the "not from VM-Entry" case, i.e. when emulating RSM or handling KVM_SET_NESTED_STATE. Failure to unwind the MMU pointer results in KVM trying to run L1 with a nested MMU, and is especially problematic if the vCPU manages to free its nested state before the VM crashes. Constructing the root for a nested EPT MMU goes through vmcs12, which is dynamically allocated/freed when nVMX is enabled/disabled. And so if the nested state is freed with the MMU still pointing at the nested MMU, KVM will hit a NULL pointer deref when attempting to get L1=>L2 EPTP. BUG: kernel NULL pointer dereference, address: 0000000000000078 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 114a2d067 P4D 111743067 PUD 11141f067 PMD 0 Oops: Oops: 0000 [#1] SMP CPU: 20 UID: 1000 PID: 1272 Comm: nested_tdp_faul Not tainted 7.3.0-rc4-8c89f11d1a99b-sink-vm #1914 PREEMPTLAZY Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 0.0.0 02/06/2015 RIP: 0010:nested_ept_get_eptp+0xb/0x10 [kvm_intel] Call Trace: <TASK> kvm_mmu_load+0xcd/0x870 [kvm] kvm_arch_vcpu_ioctl_run+0x18f5/0x1f80 [kvm] kvm_vcpu_ioctl+0x2c7/0x970 [kvm] __x64_sys_ioctl+0x90/0xd0 do_syscall_64+0x9c/0x4d0 entry_SYSCALL_64_after_hwframe+0x4b/0x53 RIP: 0033:0x47491b </TASK> Modules linked in: kvm_intel kvm irqbypass CR2: 0000000000000078 ---[end trace 0000000000000000]--- RIP: 0010:nested_ept_get_eptp+0xb/0x10 [kvm_intel] [sean: write changelog]	N/A	More Deta
CVE-2026-87878	Linux binaries have executable stack attribute enabled. The following products are affected: Acronis Cyber Protect 17 (Linux) before build 42587.	N/A	More Deta
CVE-2026-99178	In the Linux kernel, the following vulnerability has been resolved: x86/kvm: Don't consume async #PF flags on a kernel #PF in NMI context An async #PF "page not present" event arrives through the #PF vector, and its reason sits in the per-CPU apf_reason.flags until __kvm_handle_async_pf() reads and clears it. If an NMI arrives after the event is injected and before the #PF handler reads the flags, and the NMI handler itself takes a #PF, that fault reads and clears the flags belonging to the #PF it interrupted. It then finds interrupts disabled in the NMI context it interrupted, and panics: Kernel panic - not syncing: Host injected async #PF in interrupt disabled region Call Trace: <NMI> panic+0x52/0x60 __kvm_handle_async_pf+0xb0/0xb0 exc_page_fault+0x71/0xb0 asm_exc_page_fault+0x27/0x30 RIP: 0010:__get_user_nocheck_8+0x6/0x20 perf_callchain_user+0x147/0x1a0 get_perf_callchain+0x12d/0x1c0 ... perf_event_nmi_handler+0x26/0x50 exc_nmi+0xe8/0x110 RIP: 0010:asm_exc_page_fault+0x0/0x30 </NMI> The last RIP line shows the NMI landing on the first instruction of the #PF entry. perf with user call chains takes such a fault: the sampling NMI walks the user stack with __get_user(), which faults when a saved frame pointer is not a valid user address or the walk runs off the top of the stack. The same window exists when KVM, running as an L1 hypervisor with DELIVERY_AS_PF_VMEXIT, reads the flags itself after a #PF VM-exit. The NMI entry code saves and restores CR2 for this nesting, but not the async #PF reason. Andy Lutomirski described the race, with perf as the example, when async #PF delivery was reworked in 2020 [1]. Saving and clearing the flags across the NMI, next to CR2, was discussed there but not merged. Since that rework, Linux has stopped setting KVM_ASYNC_PF_SEND_ALWAYS, so the host delivers "page not present" only for user mode faults and a kernel-mode fault in NMI context (including kernel-mode #MC and #DB) cannot be an async page fault. In that case, return without touching the flags so that the interrupted handler finds them intact. Tested on v7.3-rc5 in a 4-vCPU, 2 GiB guest restored from a snapshot whose memory is served on demand through userfaultfd, so that reading it back takes async #PFs, while every thread samples hardware cycles with user call chains and points its frame pointer at an unmapped page. Without this patch the guest panicked as above in 3 of 3 runs. With it, the guest survived 3 of 3 runs of 60 seconds, and the host counted 148,441 to 153,334 kvm_async_pf_not_present events in the first 20 seconds of each. On 6.18.50 the results were the same: the guest panicked without the patch and survived with it.	N/A	More Deta
CVE-2026-99179	In the Linux kernel, the following vulnerability has been resolved: watch_queue: Fix note pool publication race in watch_queue_set_size() There is a race between watch_queue_set_size() and post_one_notification(). watch_queue_set_size() publishes wqueue->notes, notes_bitmap, nr_pages and nr_notes with plain stores, and post_one_notification() reads them with plain loads under a different lock, so nothing orders the four stores against the poster's loads: depending on the build, notes can be stored last (gcc 14 on x86-64 does this). Since keyctl_watch_key() lets a watch attach to a queue before it is sized, post_one_notification() can already be running on another CPU at that moment: it reads nr_notes > 0, passes its bounds check, and then reads notes while it is still NULL, dereferencing notes[0]. An unprivileged user triggers this reliably by watching one of its own keys through a notification pipe and racing ioctl(IOC_WATCH_QUEUE_SET_SIZE) on that pipe against keyctl(KEYCTL_SETPERM) on the key from another CPU, triggering: BUG: kernel NULL pointer dereference, address: 0000000000000000 RIP: 0010:post_one_notification.isra.0+0xa2/0x1e0 Call Trace: __post_watch_notification+0x148/0x180 keyctl_setperm_key+0x119/0x130 do_syscall_64+0x108/0x4c0 entry_SYSCALL_64_after_hwframe+0x77/0x7f Kernel panic - not syncing: Fatal exception in interrupt Fix this by publishing nr_notes last with smp_store_release(), and by reading it once with smp_load_acquire() in post_one_notification() before the bitmap and the page array are touched. A poster that observes a non-zero nr_notes then also observes the pool behind it; one that observes zero drops the notification as before.	N/A	More Deta
CVE-2026-87103	Sensitive information disclosure and manipulation due to improper token validation. The following products are affected: Acronis Cyber Protect 17 (Linux, Windows) before build 42587.	N/A	More Deta
CVE-2026-99181	In the Linux kernel, the following vulnerability has been resolved: autofs: ignore notification errors from a replaced pipe autofs_notify_daemon() takes a reference to the current notification pipe under wq_mutex, then drops the mutex before writing the request. The write can block while the daemon enters catatonic mode and installs a replacement pipe. If the old pipe's reader is then closed, the delayed write returns -EPIPE and the generic error path enters catatonic mode again. That transition acts on the current superblock state, closes the replacement pipe, and releases the new daemon generation's wait queues. Only enter catatonic mode when the pipe which failed is still the current pipe. Factor the already-locked transition so the identity check and state change are atomic with respect to another replacement. This was reproduced on v7.3-rc5-337-gff47652a4b66c in a local QEMU guest. An unprivileged UID 65534 lookup filled the old packet pipe before a normal CATATONIC/SETPIPEFD restart. On the unmodified kernel, the new pipe received HUP and both a pending victim lookup and a later lookup failed with ENOENT in two out of two fresh-mount runs. With this change, the new pipe remained active, received an intact 304-byte request, and both victim lookups completed in two out of two runs. Normal lookup and restart-without-a-blocked-writer controls passed. No KASAN, oops, refcount, or lock diagnostic was	N/A	More Deta

	observed. A source reproducer and complete local logs are available privately on request. The demonstrated impact is limited to denial of a shared autofs service during a legitimate daemon restart. No memory corruption, information leak, privilege escalation, or code execution primitive was observed.		
CVE-2026-99182	In the Linux kernel, the following vulnerability has been resolved: ASoC: SOF: ipc4-topology: Fix shift-out-of-bounds for aggregated ALH capture When ch_count is smaller than blob->alh_cfg.device_count (e.g. a mono capture stream, such as a SmartMic, aggregated across multiple SDW links), step = ch_count / blob->alh_cfg.device_count truncates to 0. The subsequent GENMASK(step - 1, 0) then underflows step - 1 (u32) to UINT_MAX, causing GENMASK()'s internal shift to use an out-of-bounds exponent: UBSAN: shift-out-of-bounds in sound/soc/sof/ipc4-topology.c:2363:13 shift exponent 18446744069414584384 is too large for 64-bit type 'long unsigned int' Treat ch_count < device_count the same way as the existing "channels equal to output reference channels" case: apply the same ch_mask to every aggregated device instead of trying to split channels that can't be evenly divided.	N/A	More Deta
CVE-2026-99151	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix NULL sink dereference in USB4 bandwidth functions allocate_usb4_bandwidth_for_stream() and allocate_usb4_bandwidth() both use ASSERT(stream->sink) before dereferencing stream->sink->link. ASSERT is compiled out in production builds, so a NULL stream->sink causes a NULL pointer dereference. link_set_dpms_off() already guards two earlier accesses to stream->sink with explicit NULL checks, confirming that stream->sink can legitimately be NULL. The subsequent call to deallocate_usb4_bandwidth() had no equivalent guard. Replace the ASSERT() calls with proper NULL checks that return false early, and add a matching stream->sink guard at the call site in link_set_dpms_off() consistent with the surrounding pattern. v2: Keep the existing ASSERT() calls for diagnostics (to report unexpected NULL sink), and add explicit NULL checks that return false before dereferencing stream->sink. Also add a matching stream->sink guard at the deallocation call site in link_set_dpms_off(). (Alex) (cherry picked from commit 98029a0ce61feb52c563f65349dd9b25f672e355)	N/A	More Deta
CVE-2026-99150	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: don't drop the runtime PM reference twice in amdgpu_gpr amdgpu_debugfs_gpr_read() drops its runtime PM reference right after reading the wave registers. When copying them to userspace fails, it jumps to the err label, which drops the reference a second time. A read into a bad buffer on Navi31 either steals a reference somebody else holds (power/runtime_usage goes from 1 to 0) or underflows the count: amdgpu 0000:03:00.0: Runtime PM usage count underflow! The registers are already in the kernel buffer at that point, so finish the hardware access first and copy the buffer with a single copy_to_user() instead of the put_user() loop with its own error path. (cherry picked from commit 31035bbd74f7c3e10c163db875b8e67f8b50ee6a)	N/A	More Deta
CVE-2026-99149	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: fix GEM object leak on ENOMEM in userptr ioctl When amdgpu_hmm_range_alloc() fails amdgpu_gem_userptr_ioctl() returns -ENOMEM right away and skips the cleanup every other error path goes through. The GEM object, the bo->parent reference on the VM root and the MMU notifier registration are all left behind. Use release_object here, not user_pages_done, range is still NULL at this point. (cherry picked from commit bbe739e407a542073ec1a7872b14843566b4919e)	N/A	More Deta
CVE-2026-99130	In the Linux kernel, the following vulnerability has been resolved: io_uring/cancel: don't spin on local work the task can't run io_uring_cancel_generic() refuses to sleep while any ring on the exiting task's tctx has local work pending. It assumes the task is that ring's submitter and that the next io_uring_try_cancel_requests() pass will run the work. This does not hold for a ring that was still IORING_SETUP_R_DISABLED when the task got its tctx node from io_uring_create() or io_ringfd_register(). The submitter is set later by IORING_REGISTER_ENABLE_RINGS, possibly from another task, and only the submitter may run local work on an IORING_SETUP_DEFER_TASKRUN ring. To the exiting task the work stays pending forever, the loop never reaches schedule(), and the task trips the WARN_ON_ONCE() once and then spins in do_exit(). An unprivileged user can set this up at will by creating a disabled ring, having a child enable it and stop, posting to the ring with IORING_OP_MSG_RING and exiting with a request in flight that only the child can complete. The exiting thread burns a CPU until the child runs or dies, and with panic_on_warn set the WARN panics the kernel. Fix by skipping the sleep only when io_allowed_defer_tw_run() allows the task to run the work. This is reasonable since work it cannot run cannot complete any of its requests either, so nothing is lost by sleeping. Drop the WARN_ON_ONCE() since handing a disabled ring to another thread is a supported scenario, not a bug state.	N/A	More Deta
CVE-2026-99114	In the Linux kernel, the following vulnerability has been resolved: ksmbd: initialize FileSystemControlFlags in FS_CONTROL_INFORMATION smb2_get_info_filesystem() reports 48 bytes for FS_CONTROL_INFORMATION, that is the whole of struct smb2_fs_control_info, but never assigns FileSystemControlFlags. Those four bytes go to the client as they are found in the response buffer. The buffer is zeroed on allocation, so a standalone request leaks nothing. A compound request can leak: the offset of the next response is advanced by the length pinned for the previous one, so a reply that was written into the buffer and then dropped in favour of the short error response of smb2_set_err_rsp() stays there, and the next reply is laid over it with only the header cleared. ksmbd does not implement quota tracking, so report no control flags.	N/A	More Deta
CVE-2026-99115	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fill in FileSysIdentifier in FS_POSIX_INFORMATION smb2_get_info_filesystem() reports 56 bytes for FS_POSIX_INFORMATION, that is the whole of FILE_SYSTEM_POSIX_INFO, but never assigns FileSysIdentifier. Those eight bytes go to the client as they are found in the response buffer. The buffer is zeroed on allocation, so a standalone request leaks nothing. A compound request can leak: the offset of the next response is advanced by the length pinned for the previous one, so a reply that was written into the buffer and then dropped in favour of the short error response of smb2_set_err_rsp() stays there, and the next reply is laid over it with only the header cleared. Report the file system id statfs() returned, which is what the field is for. FileSysIdentifier is __le64 and f_fsid is a pair of ints, so assemble the value first, val[0] as the low half, and convert it on the way out.	N/A	More Deta
CVE-2026-99111	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix data corruption with concurrent writes and O_TRUNC cifs_do_truncate() flushes dirty pages with filemap_write_and_wait() and truncates the file on the server, but in the old code both operations ran without holding i_rwsem or invalidate_lock. A concurrent buffered write via netfs_perform_write() -- which only needs i_rwsem shared -- could dirty new pages after the flush but before the local truncation, and those pages would be silently discarded by cifs_setsize() -> truncate_pagecache(). Fix by acquiring inode_lock (exclusive i_rwsem) and filemap_invalidate_lock at the top of cifs_do_truncate(), so the entire flush-truncate-resize sequence is atomic with respect to: - buffered writes (blocked by exclusive i_rwsem, since netfs_start_io_write takes i_rwsem shared), - read page faults (blocked by exclusive invalidate_lock, since filemap_fault takes it shared), - writeback collection (blocked by netfs_wb_begin/netfs_wb_end around the server truncate and local resize, since netfs_writepages also acquires the wb lock).	N/A	More Deta
CVE-2026-99118	In the Linux kernel, the following vulnerability has been resolved: drm/i915/dmc: Harden DMC firmware payload parsing Validate the conversion of the DMC firmware size from dwords to bytes using check_mul_overflow() before calculating the firmware payload size. Reject zero-length payloads and zero MMIO counts in the DMC firmware header so malformed firmware is caught early. Also set dmc_fw_size only after the payload allocation succeeds. (cherry picked from commit efde6601a1f1daedfe3dcc2816c934ddb44e3eef)	N/A	More Deta
CVE-2026-99119	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu/userq: actually validate userq BOs This was supposed to loop over the individual evicted list, as the kernel and always_valid evicted lists were already handled in amdgpu_vm_validate. Without this, BOs that were created and evicted before a userq was made would never end up in an eviction fence rearm. Also add the missing ref to the BO before drm_exec locks and refs it. (cherry picked from commit 18decfc9e8cc0fa70b6de9944cc27a37729edfbd)	N/A	More Deta
CVE-	In the Linux kernel, the following vulnerability has been resolved: KVM: x86/mmu: Cope with the SS bit being set in #NPF exit codes When running Hyper-V from Windows 11, KVM is seeing the SS bit set in nested page fault error codes produced for shadowed NPT. The AMD manual is unclear about when SS is set, including whether it can be set when SupervisorShadowStackEn (bit 6) is not set in the MISC_CTL field of the VMCB. Nevertheless, the unexpected SS bit causes out of bounds accesses in permission_fault(), seen as either WARNs or UBSAN reports: kernel: UBSAN: array-index-out-of-bounds in arch/x86/kvm/mmu.h:225:27 kernel: index 34 is out of range for type 'u16 [16]' (in this case, the page fault error code is 34*2=0x44, i.e. SS|U; the report shows SS|U|W happening as well). Fix the handling of unknown error codes by dropping SS and (with a		

2026-99120	WARN) any bits not among those that permission_fault() expects to receive. At the same time, given the uncertainty about when hardware sets SS, follow the processor's behavior when constructing the fault's error code, and preserve the SS bit as passed to FNAME(walk_addr_generic). While the behavior is surprising, there's a possibility that Hyper-V expects it (Hyper-V does not even enable CET unless it finds MBEC/GMET!), so retain the information when reflecting the fault to L1 instead of unconditionally discarding it. Bisection shows that this started happening with commit 687ee95c1b6d ("KVM: nSVM: enable GMET for guests"), even though SHSTK was available to guests since Linux 6.18. However, this is not because bit 1 of MISC_CTL (GMET) somehow enables reporting the SS bit; rather, it's simply that Hyper-V never uses CET unless GMET is also present. The WARN is reproducible even with gmet=0, with some hacking of kvm-unit-tests's cet.c testcase to ensure that the first access to the shadow stack triggers a page fault.	N/A	More Deta
CVE-2026-99121	In the Linux kernel, the following vulnerability has been resolved: ipv4: avoid divide by zero in fib_rebalance fib_rebalance() computes the total eligible nexthop weight in one pass and programs upper bounds in a second pass. A concurrent change to ignore_routes_with_linkdown can make the first pass return zero while the second pass sees an eligible nexthop, resulting in division by zero. If the first pass reports a zero total, set each nexthop upper bound to -1 and skip the division. This matches the IPv6 fix in commit d2c26c2911dd ("ipv6: avoid divide by zero in rt6_multipath_rebalance") and preserves the lock-free rebalance path.	N/A	More Deta
CVE-2026-99124	In the Linux kernel, the following vulnerability has been resolved: s390/pci: Fix leak of uninitialized kernel data in SCLP report While report_error_write() checks that the provided buffer is at least as large as the header struct, but not that it is large enough to contain the report with the length claimed by report->length. If user-space provides a short buffer, meaning a larger report->length than the actually written payload, up to around 4K of kernel data from past the kmalloc(len + 1) sized buffer allocated in kernfs_fop_write_iter() will leak into the SCLP report. However, as the entity processing the SCLP is privileged and able to access at least the page including the report, this does not leak data that entity could not access but it is still an out of bounds read and a malformed error report that should be rejected.	N/A	More Deta
CVE-2026-99125	In the Linux kernel, the following vulnerability has been resolved: s390/pai: Handle multiple PMU stop callback invocations Handle the following scenario: The kernel protects itself against a very high sampling load and throttles the sampling using: perf_event_throttle() --> PMU->stop() Shortly later the scheduler may terminate the task and removes it from the CPU. It again calls PMU->stop() which results in two invocations of PMU->stop() called back to back. Protect against this and check the PERF_HES_STOPPED bit on function entry. If it is already set return. Clear bit PERF_HES_STOPPED in PMU->start(). Prohibit ioctl(fd, PERF_EVENT_IOC_PERIOD, ...) call for this event. It sets perf_event::event_limit to a positive value and causes perf_event_overflow() to invoke pai_stop() call back function when perf_event::event_limit hits zero. This is not supported because the sample events CRYPTO_ALL and NNPA_ALL are only taken at schedule out of a task. Use list_for_each_entry_safe() for safe iteration over syswide_list in pai_have_samples().	N/A	More Deta
CVE-2026-99126	In the Linux kernel, the following vulnerability has been resolved: s390/ctcm: Prevent XID null dereference The mpc_validate_xid() function sets grp->saved_xid2->xid2_flag2 to 0x40 to signal XID validation error. If peer XID is NULL or r/w channel pairing mismatch happens, grp->saved_xid2 is never initialized. An attempt to set the flag in such case leads to NULL dereference. Fix this by using the always available priv->xid->xid2_flag2 instead of grp->saved_xid2->xid2_flag2 for validation errors.	N/A	More Deta
CVE-2026-99127	In the Linux kernel, the following vulnerability has been resolved: page_pool: keep frag_offset aligned for odd-sized requests page_pool_alloc_frag_netmem() rounds the requested fragment size with size = ALIGN(size, dma_get_cache_alignment()); dma_get_cache_alignment() returns 1 unless the architecture defines ARCH_DMA_MINALIGN, which DMA-coherent architectures such as x86 do not. There the ALIGN() is a no-op and pool->frag_offset advances by the raw, unrounded size. A single caller asking for an odd size then leaves frag_offset misaligned for every fragment carved out of that page afterwards. The pool is shared, so the damage is not confined to the caller that caused it. The per-cpu system_page_pool used by generic XDP hits this. skb_pp_cow_data() allocates its fragments with the raw packet length: size = min_t(u32, len, PAGE_SIZE); truesize = size; page = page_pool_dev_alloc(pool, &page_off, &truesize); leaving frag_offset odd for whatever is carved out of that page next. Its own head allocation is already aligned -- SKB_HEAD_ALIGN(size) plus the XDP_PACKET_HEADROOM its callers pass -- so it is a later user of the shared pool that pays: page_pool_dev_alloc_va() returns a misaligned buffer, napi_build_skb() installs it as skb->head, and skb_shinfo(skb) == skb->head + skb->end is misaligned with it. skb_shinfo()->dataref is a 4-byte atomic_t at offset 0x20, so the atomic_inc() in __skb_clone() straddles a cache line. On x86 with split lock detection -- fatal for kernel split locks by default -- this panics the machine: Oops: Split lock detected RIP: 0010:skb_clone+0x154/0x1e0 Call Trace: <IRQ> raw_local_deliver+0x1ed/0x2c0 ip_protocol_deliver_rcu+0x54/0x1c0 ip_local_deliver_finish+0x85/0x100 ip_local_deliver+0x67/0x100 __netif_receive_skb_one_core+0x85/0xa0 process_backlog+0x87/0x130 Reproduced by attaching any generic-mode XDP program to loopback and opening a RAW IPPROTO_UDP socket, which makes raw_local_deliver() clone every locally delivered UDP packet; ordinary DNS traffic then triggers it, roughly once per 2500 clones. Observed on 6.12.101 and 7.1.8. Tracing page_pool_alloc_frag_netmem() over one such run shows the amplification -- two odd-sized requests, nine misaligned offsets: requested size & 7: 0: 17035 5: 1 7: 1 frag_offset & 7: 0: 17028 3: 1 4: 1 5: 1 6: 1 7: 5 and skb_pp_cow_data() returning heads that were aligned on entry: head 0xffff8f4c86aeac00 -> 0xffff8f4c53a9a9c4 (&7=4) head 0xffff8f4d6a8a42c0 -> 0xffff8f4c4f7b7a45 (&7=5) Round the fragment size up to at least the alignment struct skb_shared_info requires, so fragments are always suitably aligned for the objects callers build on them. Architectures needing a larger DMA alignment keep it. This also makes the remainder computed in page_pool_alloc_netmem(), *size = max_size - *offset; aligned, since max_size is a power of two -- which fixes the matching misalignment of skb->end. Verified with a controlled A/B under QEMU/KVM: same tree, same config, same compiler, same rootfs and identical traffic, differing only by this patch. A SEC("xdp.frags") XDP_PASS program on lo plus UDP datagrams larger than max_head_size drives skb_pp_cow_data()'s fragment loop, which passes raw packet lengths to the pool. Measured at the return of skb_pp_cow_data(): unpatched patched skb_pp_cow_data calls 40800 40800 misaligned skb->head 1120 0 dataref at line offset >60 80 0 The last row counts the accesses that actually fault: skb_shinfo()->dataref sits at head+end+0x20 and is a 4-byte atomic, so `lock incl` splits a 64-byte cache line only when that address lands at offset 61..63. All 80 occurrences were at offset 61; the panic reported above was at offset 62. Eliminating the misalignment removes every one of them. Same class of bug as commit 3bed3cc4156e ("net: Do not allocate page fragments t ---truncated---	N/A	More Deta
CVE-2026-99128	In the Linux kernel, the following vulnerability has been resolved: sctp: validate chunk length in the inqueue parser SCTP chunks always include a four-byte generic header, but sctp_inq_pop() currently accepts shorter declared lengths. A zero-length chunk leaves chunk_end at the current header. When ASCONF is covered by the association's SCTP-AUTH policy, sctp_assoc_bh_rcv() can continue before the state machine performs its normal chunk-length check. sctp_inq_pop() then returns the same malformed chunk repeatedly and the receive softirq can lock up. A remote SCTP peer can trigger this after establishing an association on a kernel built with CONFIG_IP_SCTP and configured with net.sctp.addip_enable=1 and net.sctp.auth_enable=1. The reproducer did not require application credentials, a shared SCTP AUTH key, or net.sctp.addip_noauth_enable=1. On commit f967455fb2a5 ("seg6: reset IP6CB after IPv6 decapsulation"), one zero-length ASCONF caused repeated watchdog soft-lockup reports in a two-vCPU KVM guest. All 3 pre-trigger health probes succeeded, while 36 of 37 post-trigger probes failed. With this change, all 37 post-trigger probes succeeded and no equivalent soft-lockup signature appeared. Reject chunks shorter than the generic SCTP header at the shared inqueue parser boundary. Mark the packet for discard before either caller can continue processing it, while preserving the four-byte generic minimum. Declared-length 1 through 4 controls and kernel-generated ASCONF traffic remained healthy. The patched sctp_hello selftest passed for IPv4 and IPv6. The complete private reproducer and validation evidence are available directly to maintainers on request.	N/A	More Deta
CVE-2026-99129	In the Linux kernel, the following vulnerability has been resolved: selinux: fix BPF token permission checks Avoid multiple lookups of the bpffs creator SID using the token's file descriptor when the same information can be found via the resolved path/dentry (in selinux_bpf_token_create()) or the token itself (in selinux_bpf_map_create() and selinux_bpf_prog_load()). Not only does this simplify the code, it avoids potential TOCTOU issues if the user changes the token file descriptor passed into the kernel.	N/A	More Deta
	In the Linux kernel, the following vulnerability has been resolved: ntfs: fix FITRIM range alignment ntfs_trim_fs() aligns the start of a free extent up to the device discard granularity, but derives the discard length by aligning the original extent length down. When the free extent start is not		

CVE-2026-99108	discard-aligned, adding that length to the aligned start can extend the discard past the free extent and into allocated clusters. For example, with 4 KiB clusters and 32 KiB discard granularity, the free extent [4 KiB, 36 KiB) becomes the discard range [32 KiB, 64 KiB), so 28 KiB beyond the free extent may be discarded. Align the absolute end of the free extent down and derive the length from the two aligned endpoints. Skip extents that contain no full discard unit. Reproduced with a 4 KiB-cluster NTFS filesystem on scsi_debug configured for 32 KiB discard granularity and read-zero-after-trim. Before this change, FITRIM zeroed seven allocated 4 KiB clusters following an unaligned 32 KiB hole. With this change, the same data remains intact across FITRIM and remount.	N/A	More Deta
CVE-2026-99147	In the Linux kernel, the following vulnerability has been resolved: drm/exec: don't immediately add prelocked obj to array of locked objs When a contention is detected the drm_exec object grabs a reference to the contended object, unlocks all other objects and pre-locks the contended one before anything else. The problem is that it is possible that this pre-locked object was about to be destroyed and drm_exec is now holding the last reference to it. So we never actually see this pre-locked object again to be explicitly locked and so also never reserve a slot for a dma_fence object on it. Should the driver now use drm_exec_for_each_locked_object() to add a new fence to all locked objects we eventually see a warning or even a BUG_ON() to prevent random memory corruption. Fix this by keeping the prelocked object out of the array of locked objs until it was explicitly mentioned by the driver again. If the prelocked object is never mentioned again by the driver just unlock and drop the reference at the end of the locking loop.	N/A	More Deta
CVE-2026-99132	In the Linux kernel, the following vulnerability has been resolved: xfs: don't hold buffer locks across sync transaction commit in xfs_sync_sb_buf xfs_sync_sb_buf() holds sb/rtsb buffer locks across a synchronous xfs_trans_commit(), which flushes the CIL push workqueue internally. If shutdown occurs during the CIL push, xfs_buf_item_unpin() needs to lock these buffers to fail them, causing a deadlock: setlabel: holds buf lock -> flush_workqueue(xfs-cil) CIL push worker: xfs_buf_item_unpin -> xfs_buf_lock(same buf) Remove the xfs_trans_bhold() calls so that commit releases the buffer locks normally. After the sync commit, re-acquire the buffers via mp->m_sb_bp / mp->m_rtsb_bp for the on-disk writeback.	N/A	More Deta
CVE-2026-99133	In the Linux kernel, the following vulnerability has been resolved: net/iucv: fix the recvmsg window update iucv_sock_recvmsg() sends the HiperSockets-only AF_IUCV_FLAG_WIN without testing the transport, so on a classic z/VM socket iucv_send_ctrl() sizes the skb through a NULL iucv->hs_dev. SO_MSGLIMIT accepts 1, so msglimit / 2 is zero and one recvmsg() on its own socket is enough for an unprivileged process to take a spurious disconnect. It also calls iucv_send_ctrl() under spin_lock_bh(&message_q.lock), which allocates GFP_KERNEL inside a section the code treats as atomic. Sending outside that lock lets two recvmsg() reach afiucv_hs_send() at once, where msg_recv is sampled for the advertised window and subtracted after dev_queue_xmit() -- and sendmsg reaches that counter under lock_sock() while recvmsg holds no socket lock, so both can subtract the same value, the counter goes negative and the credit reaches the peer twice. Test the transport, claim the credit with atomic_xchg() after the last error exit and hand it back if the transmit fails, and send once the lock is dropped.	N/A	More Deta
CVE-2026-99134	In the Linux kernel, the following vulnerability has been resolved: mac802154: fix data race and NULL deref on local->assoc_dev local->assoc_dev is shared between the association path and the association-response worker without common synchronization. mac802154_perform_association() stores the coordinator pointer and waits for a response. Its timeout and error paths clear the pointer and return to mac802154_associate(), which may then free the coordinator object. Meanwhile, mac802154_rx_mac_cmd_worker() may observe the associating bit and enter mac802154_process_association_resp(), which dereferences assoc_dev. The worker's bit test and the handler's pointer dereference are not atomic with respect to cleanup. Cleanup can clear assoc_dev between them, causing a NULL dereference, or free the coordinator while the response handler still uses the pointer. The recorded result is exposed to the same window. assoc_status and assoc_addr are written by the handler but read by the association path while the associating bit is still set, so a second response for the same request - a malicious one, for instance - can replace them between those reads and leave the caller with an incoherent status and address pair. The response handler only needs the coordinator extended address. Replace assoc_dev with a cached address, removing the pointer lifetime dependency. Protect the cached address and the associating bit with a dedicated spinlock. A READ_ONCE()/WRITE_ONCE() pair would not guarantee an atomic __le64 access on all 32-bit architectures. wpan_dev->association_lock cannot be reused here: nl802154_associate() holds it across rdev_associate(), hence for the whole of mac802154_perform_association() including the wait for the response. A response handler taking that lock would only get it once the association has already given up. Reset the completion, publish the cached address, and set the associating bit while holding the lock. The response handler takes the lock, rechecks the bit and the cached address, records the response, clears the bit, and only then completes the waiter. Thus cleanup cannot pass the handler between its state check and completion, and the cached 64-bit value cannot tear. The handler clears the bit before completing, not the woken waiter: otherwise complete() is issued under the lock and a second (e.g. malicious) response can reacquire it before the waiter and replace the result. So a wait that returns success implies the bit is already clear, and the success and negative-response paths return directly. The transmit-error and timeout paths still clear it under assoc_lock, which serializes any racing response against the cleanup while the call returns the error it already selected. Both paths snapshot assoc_status and assoc_addr under the same lock. Both users run in process context, so a plain spinlock is sufficient. The lock is not held while waiting for the completion.	N/A	More Deta
CVE-2026-99135	In the Linux kernel, the following vulnerability has been resolved: dm-integrity: fix infinite loop on discard with large tag size When integrity_metadata handles a discard, it fills a buffer with DISCARD_FILLER and writes it over the tags, max_blocks blocks at a time. If the kmalloc fails, the buffer is the on-stack array checksums_onstack and max_size is set to HASH_MAX_DIGESTSIZE. So if the tag size is larger than HASH_MAX_DIGESTSIZE, max_blocks is zero, bi_size is never decremented and the loop never terminates. Fix this by using sizeof(checksums_onstack) as max_size. The array has MAX_TAG_SIZE bytes since commit b93b6643e9b5 ("dm integrity: fix a crash with unusually large tag size"), so max_blocks is at least 1.	N/A	More Deta
CVE-2026-99137	In the Linux kernel, the following vulnerability has been resolved: cifs: don't update i_size in cifs_do_truncate without a cached handle If find_writable_file() returns null, cifs_file_flush will return 0 without issuing set_file_size, and the outer 'if (!rc)' block will set i_size to 0 before telling the server to truncate. If the cifs_open() then fails, the inode will have size 0, while the server file is unchanged. Move the netfs_resize_file() and cifs_setsize() into the 'if (cfile)', so they only run after a successful set_file_size. In the no-handle else branch, evict stale pages with truncate_inode_pages before the O_TRUNC open to dispose of old cache pages, and let the open response set the i_size.	N/A	More Deta
CVE-2026-99138	In the Linux kernel, the following vulnerability has been resolved: tcp: fix use-after-free in do_tcp_getsockopt(TCP_CC_INFO) do_tcp_getsockopt() reads icsk->icsk_ca_ops and dereferences the get_info function pointer without rcu_read_lock(). With BPF struct_ops congestion control, ca_ops can point to dynamically allocated memory that is freed concurrently, resulting in a use-after-free when the kernel dereferences or calls through the stale pointer. BUG: KASAN: slab-use-after-free in do_tcp_getsockopt+0x2037/0x23e0 Read of size 8 at addr ffff888013701258 by task exploit/149 do_tcp_getsockopt+0x2037/0x23e0 (net/ipv4/tcp.c:4564) tcp_getsockopt+0x91/0xf0 __sys_getsockopt+0xf7/0x170 Fix this by wrapping the ca_ops load and get_info call within rcu_read_lock()/rcu_read_unlock(), and using READ_ONCE() to load the icsk_ca_ops pointer.	N/A	More Deta
CVE-2026-99139	In the Linux kernel, the following vulnerability has been resolved: tcp: fix use-after-free in do_tcp_getsockopt(TCP_CONGESTION) do_tcp_getsockopt() reads icsk->icsk_ca_ops->name without holding rcu_read_lock(). Since commit 0baf26b0fcd7 ("bpf: tcp: Support tcp_congestion_ops in bpf"), icsk_ca_ops can point to dynamically allocated BPF struct_ops memory that may be freed concurrently via setsockopt(TCP_CONGESTION), leading to a use-after-free. BUG: KASAN: slab-use-after-free in _copy_to_user+0x37/0x60 Read of size 16 at addr ffff888013505260 by task exploit/149 _copy_to_user+0x37/0x60 do_tcp_getsockopt+0x158a/0x2460 (net/ipv4/tcp.c:4585) tcp_getsockopt+0x91/0xf0 __sys_getsockopt+0xf7/0x170 Fix this by holding rcu_read_lock() around the ca_ops->name access, using READ_ONCE() to load icsk_ca_ops, and copying the name to a stack buffer before releasing the lock. Also annotate the relevant icsk_ca_ops stores with WRITE_ONCE() to fix the accompanying KCSAN data-race issue.	N/A	More Deta
	In the Linux kernel, the following vulnerability has been resolved: tracing: Fix hist trigger timestamps for buffered events Syzkaller triggered a WARN_ON_ONCE(!nest) warning: WARNING: kernel/trace/ring_buffer.c:821 at ring_buffer_event_time_stamp Call trace: ring_buffer_event_time_stamp hist_field_timestamp hist_fn_call event_hist_trigger event_triggers_call __event_trigger_test_discard trace_event_buffer_commit do_trace_event_raw_event_sched_switch trace_event_raw_event_sched_switch The warning is probabilistically		

CVE-2026-99140	reproducible and is related to syzkaller executing the following commands: echo 'prev_pid == 999999' > events/sched/sched_switch/filter echo 'hist:keys=common_timestamp' > events/sched/sched_switch/trigger The specific triggering process is as follows: CPU 0 CPU 1 (context switching) (echo 'hist:keys=common_timestamp' > \ events/sched/sched_switch/trigger) do_trace_event_raw_event_##call trace_event_buffer_lock_reserve if (!tr->no_filter_buffering_ref && trace_file->flags & EVENT_FILE_FL_FILTERED) return entry; // return directly event_hist_trigger_parse hist_register_trigger tracing_set_filter_buffering(file->tr, true); tr->no_filter_buffering_ref++; __trace_buffer_lock_reserve rb_start_commit local_inc(&cpu_buffer->committing); // skipped and not executed trace_event_buffer_commit __event_trigger_test_discard event_triggers_call event_hist_trigger hist_fn_call hist_field_timestamp ring_buffer_event_time_stamp nest = local_read(&cpu_buffer->committing); WARN_ON_ONCE(!nest) // trigger warning The root cause is that when an event file has a filter attached and the hist trigger has not yet been attached, trace_event_buffer_lock_reserve() writes the event into the per-CPU trace_buffered_event temp buffer instead of reserving it in the ring buffer, so cpu_buffer->committing is not incremented. When the event is later processed at commit time by a hist trigger, hist_field_timestamp() -> ring_buffer_event_time_stamp() sees a zero committing count, triggering WARN_ON_ONCE(!nest). tracing_event_time_stamp() was added by commit d8279bfc5e959 ("tracing: Add tracing_event_time_stamp() API") for exactly this case: if the event is the per-CPU trace_buffered_event, it returns the current ring buffer timestamp. But it never gained a caller. Use it in hist_field_timestamp(), so that a hist trigger that races onto a buffered event records the current time, which is only marginally later than when the event was recorded, instead of warning and recording a bogus timestamp.	N/A	More Deta
CVE-2026-99141	In the Linux kernel, the following vulnerability has been resolved: tracing: Fix crash in print_graph_function_event() tracing_set_tracer() assigns the flags of the newly selected tracer with: tr->current_trace_flags = t->flags ? : t->tracer->flags; If the new tracer defines neither static flags nor default flags, like hwlat, irqsoff or wakeup, add_tracer() has no per instance flags copy for it, and both operands are NULL, so tr->current_trace_flags ends up being NULL as well. The ring buffer is not cleared when switching tracers: it is reset inside tracer_init(), after current_trace_flags was already assigned. If the buffer still holds function_graph entries of the previous tracer, printing one of them dereferences the NULL pointer. This was hit by cat trace during an ftrace stress test: BUG: kernel NULL pointer dereference, address: 0000000000000000 #PF: supervisor read access in kernel mode RIP: 0010:print_graph_function_event+0xe/0x20 Call Trace: s_show+0x4d/0x110 seq_read_iter+0x2d4/0x490 seq_read+0x130/0x170 vfs_read+0xb5/0x370 ksys_read+0x6d/0xe0 do_syscall_64+0xbc/0x450 The snapshot buffer is not reset at all, so this can be reproduced without a race: echo function_graph > /sys/kernel/tracing/current_tracer echo 1 > /sys/kernel/tracing/snapshot echo hwlat > /sys/kernel/tracing/current_tracer cat /sys/kernel/tracing/snapshot Rather than teaching every user of tr->current_trace_flags about this corner case, make sure it is never NULL: when the newly selected tracer has no flags at all, tracing_set_tracer() falls back to a static empty no_tracer_flags. run_tracer_selftest() can hit the same case, so the same fallback is added there too. The existing users already handle opts == NULL, so these tracers keep behaving as before.	N/A	More Deta
CVE-2026-99106	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: free the userptr ranges when a CS fails after parser_bos amdgpu_cs_parser_bos() allocates an HMM range for every userptr entry of the BO list and looks up the user pages. Those ranges are only freed when amdgpu_cs_parser_bos() itself fails or when amdgpu_cs_submit() checks them under the notifier lock. If amdgpu_cs_patch_jobs(), amdgpu_cs_vm_handling(), amdgpu_cs_sync_rings() or the early part of amdgpu_cs_submit() fails, nothing frees them: neither amdgpu_cs_parser_fini() nor amdgpu_bo_list_free() touch e->range. Each such CS then leaks the range, its hmm_pfns array (8 bytes per page of the userptr BO) and the BO reference the range holds. An IB on a ring that patches the CS in place (e.g. VCN) with an unmapped va_start fails in amdgpu_cs_patch_ibs() and takes this path. Free the ranges on those error paths. Ranges amdgpu_cs_submit() already dropped are NULL, so freeing them again is a no-op. (cherry picked from commit c52a9542ed7cfd527feb938bd0accada2ac8d267)	N/A	More Deta
CVE-2026-99144	In the Linux kernel, the following vulnerability has been resolved: sched_ext: Fix use-after-free of a destroyed user DSQ by a deferred reenqueue A deferred reenqueue can read a freed user DSQ. The request stays on its CPU's deferred list until run_deferred() takes it, and the RCU callback that frees the DSQ assumes that the grace period has flushed it, so exit_dsq() checks the per-CPU node without the deferred list lock. A grace period waits for readers in flight, not for a pending run_deferred(). A run_deferred() which starts after the grace period began can detach the request right before the callback looks and then read the freed DSQ's id. Cancel the pending requests before the grace period instead. The irq work that frees the DSQ unlinks every CPU's request under the per-CPU deferred list lock, and schedule_dsq_reenq() ignores a new request under the same lock once the id is invalid. Only a run_deferred() that started before the grace period can hold a request, and it runs with IRQs disabled, so the grace period waits for it and nothing touches the DSQ after the callback.	N/A	More Deta
CVE-2026-99145	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Don't transfer shrinker pages for pinned bos on purgeable state change Pinned bos have their pages removed from the shrinker's shrinkable / purgeable counts on pin, and added back on unpin according to the bo's purgeable state at that time. However, xe_bo_set_purgeable_shrinker() unconditionally transfers pages between the shrinkable and purgeable counts. If the purgeable state of a pinned bo changes, for example by userspace madvising DONTNEED on a VMA of a bo that is also pinned as a scanout buffer, this underflows one count and, after unpin, leaves the other one permanently inflated. Only update the purgeable flag for pinned bos, and leave the page accounting to unpin. (cherry picked from commit afe6bc012034123fd838328668e609bf57e46bd3)	N/A	More Deta
CVE-2026-99146	In the Linux kernel, the following vulnerability has been resolved: drm/i915/dmc: Add sanity check for DMC load address For DMC firmware header version 3, the firmware load address is stored in dmc_info->start_mmioaddr and later used by dmc_load_program(). Unlike the MMIO address table, the firmware load address is not validated. Add a sanity check to ensure it is within the valid range. BSpec: 69671, 68378 (cherry picked from commit 5e47ee5c76ca9becde8df4ad5202845b7ffcbc4c)	N/A	More Deta
CVE-2026-99183	In the Linux kernel, the following vulnerability has been resolved: accel/rocket: search every core slot when looking up a scheduler sched_to_core() walks rdev->cores[] up to rdev->num_cores, and rocket_remove() decrements num_cores for every core it removes. Unbind a core that is not the last one and the cores behind it fall outside the search, so sched_to_core() returns NULL for a core that is still bound and still running jobs. Neither caller checks the result: rocket_job_run(): rocket_fence_create(core), core->dev rocket_job_timedout(): dev_err(core->dev, "NPU job timed out") Unbinding the middle core of the three on an RK3588 while three clients are submitting to all of them faults twice, once from the surviving core's job queue and once from its reset work: KASAN: null-ptr-deref in range [0x0000000000000220-0x0000000000000227] Workqueue: fdad0000.npu drm_sched_run_job_work [gpu_sched] pc : rocket_job_run+0x234/0x838 [rocket] Call trace: rocket_job_run+0x234/0x838 [rocket] drm_sched_run_job_work+0x2cc/0xad8 [gpu_sched] process_one_work+0x640/0x14f0 KASAN: null-ptr-deref in range [0x0000000000000000-0x0000000000000007] Workqueue: rocket-reset-2 drm_sched_job_timedout [gpu_sched] pc : rocket_job_timedout+0xf0/0x1e0 [rocket] Call trace: rocket_job_timedout+0xf0/0x1e0 [rocket] drm_sched_job_timedout+0x188/0x6a0 [gpu_sched] Both are the third core: the workqueue names are its device and its core->index, and it was left at slot 2 while num_cores had dropped to 2. Search all the slots that were allocated, the way find_core_for_dev() now does. A core that is still bound is then found, and the two callers get the pointer they already assume they have. This does not make unbinding one core out of several safe. An open client keeps an entity pointing at the scheduler of the core that went away: drm_sched reports it as not ready for every job that lands on it, and the client waits in dma_fence_default_wait for a fence that will never signal. Stopping the NULL dereference is what belongs in a fix; the rest wants more thought.	N/A	More Deta
CVE-2026-	In the Linux kernel, the following vulnerability has been resolved: accel/rocket: search every core slot when a core is removed rocket_remove() decrements rdev->num_cores for each core it removes, while find_core_for_dev() searches slots 0 to num_cores - 1. Unbinding the cores in the order they were bound therefore loses the last one: by the time it is removed the search range has already shrunk past its slot, so find_core_for_dev() returns -1 and rocket_remove() gives up without doing anything. num_cores never reaches zero, rocket_device_fini() never runs, and the file-scoped rdev keeps pointing at a device that is going away. Binding the cores again starts from that stale count, because rocket_probe() takes rdev->num_cores as the slot to fill. On an RK3588, which describes three cores, the second round lands on slots 1, 2 and 3 while rdev->cores was allocated with room for three: rocket fdab0000.npu: Rockchip NPU core 1 version: 1179210309 rocket fdac0000.npu: Rockchip NPU core 2 version: 1179210309 rocket fdad0000.npu: Rockchip NPU core 3 version: 1179210309 The write to rdev->cores[3] is past the end of the array. Nothing in tree reads the core array often enough to notice, so the overrun is silent today. It turned up while testing a devfreq series on top of this, where a worker walks every core a few times a second, and UBSAN caught the first bool it read out of the overrun entry:	N/A	More Deta

99184	UBSAN: invalid-load in drivers/accel/rocket/rocket_devfreq.c:47:10 load of value 5 is not a valid value for type '_Bool' Workqueue: devfreq_wq devfreq_monitor Record how many slots were allocated and search all of them. Every core is then found on removal, num_cores reaches zero, the device is torn down and a later bind starts from a clean rdev. This does not make unbinding a single core out of several work. probe still takes num_cores as the slot to fill, so rebinding one core while its siblings stay bound would write over a slot that is already in use, and rocket_open() still reaches for cores[0] whether or not anything is there. Both of those want more thought than a fix should carry. Found by unbinding and rebinding all three cores on an Orange Pi 5 Plus. With this applied, 25 unbind/rebind rounds and 5 module unload/reload rounds run clean there: the cores land in slots 0, 1 and 2 every time, whichever order they are bound in, and the shared supply goes back to a single user after each round.		
CVE-2026-87102	Sensitive information disclosure and manipulation due to improper token validation. The following products are affected: Acronis Cyber Protect 17 (Linux, Windows) before build 42587.	N/A	More Deta
CVE-2026-117849	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-87097	Sensitive information disclosure due to insufficiently protected credentials. The following products are affected: Acronis Cyber Protect 17 (Linux, Windows) before build 42587.	N/A	More Deta
CVE-2026-117858	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117857	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117856	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117855	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117854	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117853	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117852	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117851	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-93515	A use-after-free in present_clear_window_notifies() in the X.org X Server before 21.1.25 and X Wayland before 24.1.14 could be used by malicious X clients to crash or potentially execute code in the X server context.	N/A	More Deta
CVE-2026-105420	Wing FTP Server does not verify user's base folder. An attacker with admin privileges can add user directories via scripts, allowing the added directories to escape the base folder. This allows the attacker to write files on the system and can lead to remote code execution with process owner privileges.Critically, since the installation guide mentions running the command with `sudo`, the files are created as “root.” This issue was fixed in version 8.2.6.	N/A	More Deta
CVE-2026-117850	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-116078	Allocation of Resources Without Limits or Throttling vulnerability in the HTTP/2 request body reader of mtrudel bandit allows an unauthenticated remote attacker to exhaust server memory via a request body sent as many 1-byte DATA frames. do_read_data/5 in lib/bandit/http2/stream.ex keeps every DATA frame payload as its own list element until the read returns. The :length option of read_body/2 counts body bytes, not frames, so a body of 1-byte frames costs a list cell and a binary term per byte. Interleaving the frames across up to 500 concurrent streams per connection keeps each stream consuming its frames as they arrive; in the reporter's test, 100 streams held 25 to 40 MiB of stream process memory for 5 MB sent. Only routes whose Plug reads the request body are affected, which includes any route behind Plug.Parsers. This issue affects bandit: from 0.3.1 before 1.14.1.	N/A	More Deta
CVE-2026-117848	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-102799	Joomla Extension - icagenda.com - CSV formula injection in the registrations export in iCagenda 3.5.0 to 4.0.16	N/A	More Deta
CVE-2026-117847	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More

117846			Deta
CVE-2026-117845	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117844	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-59959	SAIL is a cross-platform library for loading and saving images with support for animation, metadata, and ICC profiles. Prior to version 1.0.2, the built-in WebP decoder can crash during loader initialization when processing a malformed animated WebP file with inconsistent container or `ANMF` frame metadata. In `sail_codec_load_init_v8_webp()` in `src/sail-codecs/webp/webp.c`, `WebPDemuxGetI` with `WEBP_FF_CANVAS_WIDTH` can return a zero `image_local->width`, which is then used as a divisor when calculating `bytes_per_pixel` from the image row size. The division happens before frame decoding and before generic image skeleton validation in `src/sail/sail_advanced.c`, causing an arithmetic fault and process termination. Applications accepting untrusted WebP images can consequently suffer denial of service; builds must include the affected WebP codec. This issue is fixed in version 1.0.2.	N/A	More Deta
CVE-2026-93517	A heap buffer overflow in handling GLX RenderLarge request where dataBytes exceeds cmdlen in X.org X server before 21.1.25 and XWayland before 24.1.14 that could be be triggered by an authenticated X client could cause crashes or code execution in X server context.	N/A	More Deta
CVE-2026-117843	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117842	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-115402	OpenVPN ovpn-dco-win 0.6.5 through 2.8.13 allows unprivileged local users to cause a denial of service (system crash) via a race condition in the TCP connect path.	N/A	More Deta
CVE-2026-117841	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117840	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117839	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117838	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-87098	Sensitive information disclosure due to improper authorization. The following products are affected: Acronis Cyber Protect 17 (Linux, Windows) before build 42587.	N/A	More Deta
CVE-2026-102790	Joomla Extension - icagenda.com - Stored XSS via url-type event Custom Field in iCagenda 3.2.1 to 4.0.16	N/A	More Deta
CVE-2026-99186	In the Linux kernel, the following vulnerability has been resolved: x86/insn-eval: Fix shadowed segment index in get_seg_reg_override_idx() Commit 45e1dccc0653 ("x86/insn: Simplify for_each_insn_prefix()") made for_each_insn_prefix() declare its own loop counter named idx. get_seg_reg_override_idx() keeps its result in a local of the same name, so the assignments in the loop body now write the loop counter: - the function always returns INAT_SEG_REG_DEFAULT, so FS and GS overrides are ignored; - a CS override sets the counter to INAT_SEG_REG_CS (2), the increment makes it 3, and prefixes.bytes[3] holds the last prefix, 0x2e again, so the loop never terminates. The UMIP emulation reaches this from the #GP handler for user space: an SGDT, SIDT or SMSW with a memory operand and a CS prefix leaves the task spinning in the kernel, never returning to user space, with a SIGKILL that is never delivered. Any user can thus tie up CPUs until reboot. With an FS or GS prefix, the emulated result is written to the wrong address. Rename the internal macro iterator variable. [Lukas' original patch renamed the use site, I changed it to rename the iterator in the macro instead, but left Lukas' commit message and authorship - Linus]	N/A	More Deta
CVE-2026-99200	In the Linux kernel, the following vulnerability has been resolved: net: hisilicon: hisi_femac: Move setting of netops to fix crash hisi_femac_drv_probe() connects the PHY before dev->netdev_ops is assigned. phy_attach_direct() -> phy_link_topo_add_phy() reads dev->netdev_ops through netdev_need_ops_lock() since the commit in question, so probing crashes with a NULL pointer dereference when CONFIG_NET_SHAPER is enabled. phy_link_topo_add_phy from phy_attach_direct+0xec/0x37c of_phy_get_and_connect from hisi_femac_drv_probe+0x1f4/0x558 Kernel panic - not syncing: Attempted to kill init! exitcode=0x0000000b Assign netdev_ops before the PHY attach, as was done for emac in commit 7c9f391ec89c ("net: emac: move setting of netops to fix crash").	N/A	More Deta
CVE-2026-99187	In the Linux kernel, the following vulnerability has been resolved: perf: Fix perf_pmu_migrate_context() leaving events behind __perf_pmu_remove() walks the group leaders of a CPU and PMU with perf_event_groups_for_cpu_pmu(), removing each one as it goes. perf_remove_from_context() takes the leader out of the groups rbtree, after which rb_next() on that node returns NULL, prematurely ending the walk. Other groups stay behind in the source context. On CPU hotplug, they are then torn down with the dying CPU. They keep running until teardown, while the PMU's interrupt and migrated events are on a new CPU, which drivers rely on never happening. Walk ctx->event_list instead and pick out the PMU's events by their pmu_ctx.	N/A	More Deta
CVE-	In the Linux kernel, the following vulnerability has been resolved: net: stmmac: dwmac1000: clear the RGMII status interrupt Since commit 2e2c878a3141 ("net: stmmac: remove SGMII/RGMII/SMII interrupt handling") nothing on the RGMII path reads GMAC_RGSMIIIS, so RGSMIIIS stays pending behind GMAC_INT_MASK from the first link change on. stmmac_resume() resets the MAC in stmmac_hw_setup(); the reset sets GMAC_INT_MASK to 0 until dwmac1000_core_init() writes the mask again, and the pending status storms the line: dwmac_dma_interrupt: unexpected status 04000000 A register dump at the first message on ODROID-HC4 showed it: core int_status 00000001 int_mask 00000000 pmt		

2026-99188	00000000 rgsmiiis 0000000d When the resume thread runs on the CPU that takes the MAC interrupt, the storm starves it: a soft lockup, then a watchdog reset or a hang. Read GMAC_RGSMIIIS in dwmac1000_irq_status() when the status is not masked, as the driver did before 2e2c878a3141; the read clears it. Wake-on-LAN resume from s2idle with the resume thread and the MAC interrupt on one CPU: Helios64 (dwmac-rk), 7.3-rc6, soft-locked in 3 of 3 resumes without a fix and in 0 of 10 with this patch; it ran with an out-of-tree dwmac-rk change that keeps the GMAC powered across suspend. ODROID-HC4 (dwmac-meson8b): 0 of 10 with this patch, 2 of 2 without a fix on a 7.3-rc5 build. irq_rgmii_n went up by one per resume.	N/A	More Deta
CVE-2026-99189	In the Linux kernel, the following vulnerability has been resolved: gpio: mxc: fix race between chained IRQ handler install and probe completion mxc_update_irq_chained_handler() is called before the IRQ domain, the generic IRQ chip, and the port list entry are set up. If an interrupt arrives in that window: - mx3_gpio_irq_handler() calls generic_handle_domain_irq() with port->domain still NULL. - mx2_gpio_irq_handler() walks mxc_gpio_ports, but the port has not been added to the list yet. Additionally, if any of the subsequent probe steps (gpio_generic_chip_init(), devm_gpiochip_add_data(), irq_domain_create_legacy(), or mxc_gpio_init_gc()) fail, the error paths never unregister the chained handler, leaving a dangling handler that points at freed memory. Move the handler installation after all its dependencies are ready and after list_add_tail(), so the handler is never live while the data structures it touches are incomplete, and is never installed if probe fails.	N/A	More Deta
CVE-2026-99190	In the Linux kernel, the following vulnerability has been resolved: gpiolib: fix memory leak in gpiod_set_array_value_complex() on error paths A drive-by review by Sashiko reports that, after a failed call to gpiochip_set_multiple(), gpiod_set_array_value() returns abruptly, bypassing the freeing of possibly alloced bitmaps, potentially leaking memory. It is an unlikely error path, but is possible. Defer the return code check until after the bitmap_free() block.	N/A	More Deta
CVE-2026-99191	In the Linux kernel, the following vulnerability has been resolved: calipso: keep BIG TCP payload_len in calipso_skbuff_setattr() calipso_skbuff_setattr() adjusts payload_len by the length of the option it inserts or resizes: payload = ntohs(ip6_hdr->payload_len); ip6_hdr->payload_len = htons(payload + len_delta); GRO can build BIG TCP packets larger than IPV6_MAXPLEN, and stores payload_len == 0 for them; ipv6_payload_len() then falls back to skb->len. For such a packet forwarded to a destination mapped to CALIPSO, the code above writes len_delta (or 65536 + len_delta when shrinking) into payload_len, and ipv6_payload_len() no longer falls back to skb->len. nf_tables, conntrack and sch_cake rely on it. The same arithmetic also wraps when a packet grows past IPV6_MAXPLEN, and a BIG TCP packet that shrinks below IPV6_MAXPLEN should get its real length back. Set payload_len from the skb length with ipv6_set_payload_len(), which stores 0 above IPV6_MAXPLEN and the real length otherwise, as ipv6_gro_complete() does. The network header was just reset to skb->data, so skb->len - sizeof(*ip6_hdr) is the payload length. Tested on one kernel (arm64, QEMU) with SELinux permissive, a minimal mdp-generated policy (network_peer_controls=1), "netlabelctl calipso add pass doi:16" and a NetLabel mapping of fd00:2::/64 to CALIPSO DOI 16. calipso_skbuff_setattr() was called through netlbl_skbuff_setattr() from a test-only debugfs hook (not part of this patch) adding a level-only label; payload_len after the call: case before fix after fix real length 1000, unlabeled 1016 1016 1016 70000 GSO, payload_len 0 16 0 70016 65530 GSO, grows past MAXPLEN 10 0 65546 65540 GSO with a 24 byte hop header, shrinks below MAXPLEN 65528 65532 65532 1000 with a 24 byte hop header 992 992 992 (0 means ipv6_payload_len() returns the real length.) On the forward path, with a client injecting unlabeled UDP through a router to a server, the router adds the CALIPSO option and the server delivers all datagrams (Udp6InDatagrams 5, Ip6InTruncatedPkts 0) with this patch.	N/A	More Deta
CVE-2026-99192	In the Linux kernel, the following vulnerability has been resolved: net: bcmgenet: unshare the skb before writing the control block bcmgenet stores first_cb, last_cb and bytes_sent in the skb control block and reads them back on completion to free the skb and credit BQL. ether_setup() leaves IFF_TX_SKB_SHARING set, so the stack can resubmit a shared skb that is still in the ring. The next transmit overwrites last_cb, so the earlier slots complete without crediting their bytes and BQL stalls the queue until the watchdog resets it. Unshare the skb before writing the control block. Reproduce with pktgen in clone_skb mode, which hands the driver the same skb while earlier copies are still in the ring: modprobe pktgen pg=/proc/net/pktgen echo "add_device eth0" > $pg/kpktgend_0 echo "dst_mac AA:BB:CC:DD:EE:FF" > $pg/eth0 echo "dst 192.0.2.1" > $pg/eth0 echo "clone_skb 8" > $pg/eth0 echo "count 0" > $pg/eth0 echo start > $pg/pgctrl & sleep 5 echo stop > $pg/pgctrl wait cat /sys/class/net/eth0/queues/tx-0/byte_queue_limits/inflight inflight stays nonzero on the now idle queue. clone_skb 0 leaves it at zero.	N/A	More Deta
CVE-2026-99193	In the Linux kernel, the following vulnerability has been resolved: net: ti: icssm-prueth: Move setting of netops to fix crash icssm_prueth_netdev_init() calls of_phy_get_and_connect() before ndev->netdev_ops is assigned. phy_attach_direct() -> phy_link_topo_add_phy() reads dev->netdev_ops through netdev_need_ops_lock() since the commit in question, so probing crashes with a NULL pointer dereference when CONFIG_NET_SHAPER is enabled. Assign netdev_ops before the PHY attach, as was done for emac in commit 7c9f391ec89c ("net: emac: move setting of netops to fix crash").	N/A	More Deta
CVE-2026-99194	In the Linux kernel, the following vulnerability has been resolved: net: ethernet: aeroflex: move setting of netops to fix crash greth_of_probe() calls greth_mdio_init(), which connects the PHY, before dev->netdev_ops is assigned. phy_attach_direct() -> phy_link_topo_add_phy() reads dev->netdev_ops through netdev_need_ops_lock() since the commit in question, so probing crashes with a NULL pointer dereference when CONFIG_NET_SHAPER is enabled. Assign netdev_ops before the PHY attach, as was done for emac in commit 7c9f391ec89c ("net: emac: move setting of netops to fix crash").	N/A	More Deta
CVE-2026-99195	In the Linux kernel, the following vulnerability has been resolved: net: ethoc: move setting of netops to fix crash ethoc_probe() calls ethoc_mdio_probe(), which connects the PHY, before netdev->netdev_ops is assigned. phy_attach_direct() -> phy_link_topo_add_phy() reads dev->netdev_ops through netdev_need_ops_lock() since the commit in question, so probing crashes with a NULL pointer dereference when CONFIG_NET_SHAPER is enabled. Assign netdev_ops before the PHY attach, as was done for emac in commit 7c9f391ec89c ("net: emac: move setting of netops to fix crash").	N/A	More Deta
CVE-2026-99196	In the Linux kernel, the following vulnerability has been resolved: net: au1000: move setting of netops to fix crash au1000_probe() calls au1000_mii_probe(), which connects the PHY, before dev->netdev_ops is assigned. phy_attach_direct() -> phy_link_topo_add_phy() reads dev->netdev_ops through netdev_need_ops_lock() since the commit in question, so probing crashes with a NULL pointer dereference when CONFIG_NET_SHAPER is enabled. Assign netdev_ops before the PHY attach, as was done for emac in commit 7c9f391ec89c ("net: emac: move setting of netops to fix crash").	N/A	More Deta
CVE-2026-99197	In the Linux kernel, the following vulnerability has been resolved: net: mv643xx: move setting of netops to fix crash mv643xx_eth_probe() connects the PHY before dev->netdev_ops is assigned. phy_attach_direct() -> phy_link_topo_add_phy() reads dev->netdev_ops through netdev_need_ops_lock() since the commit in question, so probing crashes with a NULL pointer dereference when CONFIG_NET_SHAPER is enabled. Assign netdev_ops before the PHY attach, as was done for emac in commit 7c9f391ec89c ("net: emac: move setting of netops to fix crash").	N/A	More Deta
CVE-2026-99198	In the Linux kernel, the following vulnerability has been resolved: net: ethernet: actions: Move setting of netops to fix crash owl_emac_probe() calls owl_emac_phy_init(), which connects the PHY, before netdev->netdev_ops is assigned. phy_attach_direct() -> phy_link_topo_add_phy() reads dev->netdev_ops through netdev_need_ops_lock() since the commit in question, so probing crashes with a NULL pointer dereference when CONFIG_NET_SHAPER is enabled. Assign netdev_ops before the PHY attach, as was done for emac in commit 7c9f391ec89c ("net: emac: move setting of netops to fix crash").	N/A	More Deta
CVE-2026-99199	In the Linux kernel, the following vulnerability has been resolved: net: hisilicon: hip04_eth: Move setting of netops to fix crash hip04_mac_probe() calls of_phy_connect() before ndev->netdev_ops is assigned. phy_attach_direct() -> phy_link_topo_add_phy() reads dev->netdev_ops through netdev_need_ops_lock() since the commit in question, so probing crashes with a NULL pointer dereference when CONFIG_NET_SHAPER is enabled. Assign netdev_ops before the PHY attach, as was done for emac in commit 7c9f391ec89c ("net: emac: move setting of netops to fix crash").	N/A	More Deta

CVE-2026-99201	In the Linux kernel, the following vulnerability has been resolved: netlink: avoid hashing the network namespace pointer The netlink rhashtable key includes a raw struct net pointer and a user-controlled port ID. Both /proc/net/netlink and socket diagnostics expose the table's bucket order. By binding and rebinding chosen NETLINK_USERSOCK port IDs, an unprivileged reader can distinguish equal buckets and recover the low bits of the Jenkins hash. Its 32-bit seed and the limited set of kernel-image slides can then be searched offline to recover the address of init_net. Use the namespace's unique, non-address net_cookie in the comparison key instead. It is assigned before the per-net initializers run and remains unchanged for the namespace's lifetime. The lookup key and object hash are still built by netlink_compare_arg_init(), keeping lookup, insertion, removal and rehashing consistent while preserving namespace separation. Neither public table walker needs to change. Reading the socket's namespace cookie in netlink_compare() is safe under RCU, including during namespace teardown. netlink_release() removes the socket from the hash table and defers its final put with call_rcu(). cleanup_net() runs the per-net exit methods and waits for outstanding RCU callbacks with rcu_barrier() before freeing namespace storage. Unlike ns.ns_id, net_cookie is also available and initialized during setup_net() in older stable kernels, making the change straightforward to backport to v5.15 and later.	N/A	More Deta
CVE-2026-87099	Cross-site scripting (XSS) vulnerability due to improper input validation. The following products are affected: Acronis Cyber Protect 17 (Linux, Windows) before build 42587.	N/A	More Deta
CVE-2026-99202	In the Linux kernel, the following vulnerability has been resolved: scsi: libsas: Fix SMP IO deadlock during HA resume smp_execute_task_sg() calls pm_runtime_get_sync() on the host before issuing an SMP command. When that command is itself issued from the HA resume path, the get_sync() deadlocks: it waits for the ongoing resume (the device is RPM_RESUMING), while the resume is blocked in sas_drain_work() waiting for that same SMP IO to complete. The deadlock needs an expander-attached SATA disk. During sas_resume_ha() -> sas_drain_work(), DISCE_RESUME -> sas_resume_sata() -> ata_sas_port_resume() requests ATA_EH_RESET, and the hard reset for such a disk is done via SMP PHY CONTROL (sas_ata_hard_reset() -> sas_phy_reset() -> sas_smp_phy_control() -> smp_execute_task_sg()). Direct-attached SATA resets through lldd_control_phy() and SSP devices use TMFs, so neither hits this. Replace the get_sync()/put_sync() pair with pm_runtime_get_noresume()/pm_runtime_put(). smp_execute_task_sg() only needs to hold off autosuspend while the SMP is in flight, and it must not try to resume the host: a sync resume issued from the HA resume path itself is what deadlocks, and by the time sas_resume_ha() runs, hw_init has already reinitialized the hardware, so the device is accessible without one. The usage reference is still required. Discovery work normally runs inside an event worker's PM reference, taken at sas_notify_port_event() notify time and held until the handler has flushed the disco queue. sas_rediscover_ex_phy() however requeues DISCE_REVALIDATE_DOMAIN from within the revalidation worker itself, and flush_workqueue() does not wait for work items queued during execution, so that chained revalidation runs with no outer PM reference - without the get_noresume(), its SMP could race autosuspend. For the BSG path, sas_smp_handler() is the only caller which may find the host autosuspended: expander SMP requests do not go through any SCSI device request queue, so nothing else in that path holds the host awake. Resume it there with pm_runtime_resume_and_get() and check the result.	N/A	More Deta
CVE-2026-87101	Sensitive information disclosure due to improper token validation. The following products are affected: Acronis Cyber Protect 17 (Linux, Windows) before build 42587.	N/A	More Deta
CVE-2026-99204	In the Linux kernel, the following vulnerability has been resolved: ocfs2/dlm: Protect the recovery list during debugfs reads Recovery participant records must remain alive while debug_state_print() walks reco.node_data and formats their fields. The formatter holds dlm->spinlock, but the recovery participant list is protected by dlm_reco_state_lock. In particular, dlm_destroy_recovery_area() detaches the list under dlm_reco_state_lock and frees the detached records after releasing it. A concurrent debugfs open can therefore read freed memory. Protect the participant traversal and field reads in debug_state_print() with dlm_reco_state_lock, matching the existing list writers. This also serializes the traversal against list_add_tail() during recovery-area initialization. Make the existing lock available to the debug code through dlmcommon.h; the lock remains internal to the OCFS2 DLM module. Release dlm->spinlock after formatting the other domain state and before acquiring dlm_reco_state_lock, so the debug reader does not nest the two locks. Leave recovery list insertion, detachment and freeing unchanged. KASAN report as below: BUG: KASAN: slab-use-after-free in debug_state_open+0x1169/0x12d0 Read of size 4 at addr ffff88810662ef80 by task dlm-state-stres/896 CPU: 1 UID: 0 PID: 896 Comm: dlm-state-stres Not tainted 7.3.0-rc4-next-20260921-pmb-ocfs2-functional-v1+ #1 PREEMPT(lazy) Hardware name: QEMU Ubuntu 24.04 PC v2 (i440FX + PIIX, arch_caps fix, 1996), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 Call Trace: <TASK> dump_stack_lvl+0x93/0xd0 print_report+0xce/0x630 ? debug_state_open+0x1169/0x12d0 ? srso_alias_return_thunk+0x5/0xfbef5 ? __virt_addr_valid+0x20e/0x420 ? debug_state_open+0x1169/0x12d0 kasan_report+0xe0/0x110 ? debug_state_open+0x1169/0x12d0 debug_state_open+0x1169/0x12d0 ? __pfx_debug_state_open+0x10/0x10 full_proxy_open_regular+0x193/0x310 do_dentry_open+0x595/0x12d0 ? __pfx_full_proxy_open_regular+0x10/0x10 vfs_open_consume+0xd1/0x400 ? srso_alias_return_thunk+0x5/0xfbef5 path_openat+0x18d0/0x2020 ? __pfx_path_openat+0x10/0x10 do_file_open+0x21e/0x470 ? __pfx_do_file_open+0x10/0x10 ? _raw_spin_unlock+0x23/0x40 ? srso_alias_return_thunk+0x5/0xfbef5 ? alloc_fd+0x3a6/0x6b0 do_sys_openat2+0xf4/0x1b0 ? __pfx_do_sys_openat2+0x10/0x10 ? srso_alias_return_thunk+0x5/0xfbef5 ? __fput+0x5b5/0xa60 __x64_sys_openat+0x136/0x1e0 ? __pfx___x64_sys_openat+0x10/0x10 do_syscall_64+0x114/0x620 entry_SYSCALL_64_after_hwframe+0x77/0x7f [Register dump omitted.] </TASK> Allocated by task 880: kasan_save_stack+0x33/0x60 kasan_save_track+0x14/0x30 __kasan_kmalloc+0xaa/0xb0 __kmalloc_cache_noprof+0x28d/0x610 dlm_remaster_locks+0x147/0x1d90 dlm_do_recovery+0xde1/0x1580 dlm_recovery_thread+0x109/0x300 kthread+0x351/0x460 ret_from_fork+0x659/0x940 ret_from_fork_asm+0x1a/0x30 Freed by task 880: kasan_save_stack+0x33/0x60 kasan_save_track+0x14/0x30 kasan_save_free_info+0x3b/0x60 __kasan_slab_free+0x5f/0x80 kfree+0x308/0x580 dlm_destroy_recovery_area+0x285/0x460 dlm_remaster_locks+0x17c4/0x1d90 dlm_do_recovery+0xde1/0x1580 dlm_recovery_thread+0x109/0x300 kthread+0x351/0x460 ret_from_fork+0x659/0x940 ret_from_fork_asm+0x1a/0x30 The buggy address belongs to the object at ffff88810662ef80 which belongs to the cache kmalloc-32 of size 32 The buggy address is located 0 bytes inside of freed 32-byte region [ffff88810662ef80, ffff88810662efa0) [Page and memory-state dumps omitted.]	N/A	More Deta
CVE-2026-99205	In the Linux kernel, the following vulnerability has been resolved: sched/core: Call wakeup_preempt() for queued tasks during class change Paul reported recent RCU changes exposed a lost resched where CPU idles with a rcutorture thread waiting while being completely runnable. Dumping the rq state at the time of idling with runnable tasks showed the following: rq->next_class = &fair_sched_class rq->nr_running = 1 rq->cfs.h_nr_queued = 0 rq->rt.rt_nr_running = 1 Although the waiting task was an RT task, "rq->next_class" did not point to rt_sched_class and was stuck at the lower priority fair_sched_class. Inspecting sched_change_end() revealed the following race with __sched_setscheduler() for queued, but non-running tasks: CPU0 CPU1 ==== ==== __schedule() /* * rq->donor is a fair task that blocks. * rq->next_class = &fair_sched_class */ rq_lock(rq0) pick_next_task() /* nr_running = 0 */ pick_task_fair() sched_balance_newidle() raw_spin_rq_unlock(rq0) rq_lock(rq0) activate_task(rq0, p) /* p is a fair task */ rq0->nr_running++; rq0->cfs.h_nr_queued++; wakeup_preempt(rq, p) rq->next_class = &fair_sched_class resched_curr() rq_unlock(rq0) __sched_setscheduler(p) /* p is moved to SCHED_RR */ task_rq_lock(p) sched_change_begin() rq0->cfs.h_nr_queued--; rq0->rt.rt_nr_running++; sched_change_end() /* * p->on_rq = 1 (ctx->queued) * but p is not rq->donor * (!ctx->running) hence * resched_curr() is and * rq->next_class upgrade is * skipped. */ task_rq_unlock() raw_spin_rq_lock(rq0) /* * rq->nr_running = 1 * rq->cfs.h_nr_queued = 0 * rq->rt.rt_nr_running = 1 * rq->next_class = &fair_sched_class */ if (rq->cfs.h_nr_queued && ...) /* Above is false */ if (rq_modified_above(this_rq, &fair_sched_class)) /* Also false since rq->next_class is still fair */ /* * sched_balance_newidle() is considered to * have failed to pull any fair tasks and no * other wakeups were detected. */ return NULL; /* pick_task_fair() */ pick_task_idle() return rq->idle; next = rq->idle; /* Preemption indicators are lost */ clear_tsk_need_resched(prev); clear_preempt_need_resched(); rq->curr = rq->idle; !!! rq->idle switches in with rq->running == 1 but !need_resched() !!! In simple words, enqueue, followed by a class change of the newly queued task goes unnoticed in rq->next_class indicator and sched_balance_newidle() sees no fair task, nor any higher priority task enqueued. The above sequence will lead to CPU idling with a runnable task on the CPU. Call wakeup_preempt() for ctx->queued cases in sched_change_end() to re-evaluate rq->next_class after class change (ENQUEUE_CLASS) and set the NEED_RESCHED indicator accordingly. Newidle balance will correctly see an enqueue of a higher priority t --- truncated---	N/A	More Deta

CVE-2026-99206	In the Linux kernel, the following vulnerability has been resolved: scsi: target: iscsi: Fix race in discovery auth updates Separate configfs opens can concurrently update the discovery AuthMethod parameter. Both callers may free the same value in iscsi_update_param_value(), causing a double-free. Protect the lookup and replacement with the discovery TPG access lock, as used by the other TPG configfs parameter updates.	N/A	More Deta
CVE-2026-99207	In the Linux kernel, the following vulnerability has been resolved: scsi: target: Disable interrupts while holding delayed_cmd_lock target_do_delayed_work() takes dev->delayed_cmd_lock with a plain spin_lock(). It runs from system_percpu_wq, so interrupts stay enabled while the lock is held. Every other acquisition of that lock uses spin_lock_irqsave(): target_handle_task_attr() and transport_complete_ordered_sync() in target_core_transport.c, and target_non_ordered_release() in target_core_device.c. That was safe while every caller of transport_complete_task_attr() ran in process context: target_complete_ok_work() from target_completion_wq, transport_complete_qf() from dev->qf_work_queue, and transport_generic_request_failure() from the submit and execute paths. Since commit 06933066d88a ("scsi: target: Add support for completing commands from backend context") that is no longer true. With complete_type=1 on a fabric that sets direct_compl_supp, target_complete() runs target_complete_ok_work() inline in the backend's completion context, which target_complete_cmd_with_sense() documents as "May be called from interrupt context". For iblock that is the bio end_io. target_complete_ok_work() starts with transport_complete_task_attr(), which takes delayed_cmd_lock in two ways: - Every ORDERED command is put on dev->delayed_cmd_list by target_handle_task_attr() and dispatched from there by target_do_delayed_work(), which marks it SCF_TASK_ORDERED_SYNC. Its completion therefore goes through transport_complete_ordered_sync(). - A SIMPLE command that completes while an ORDERED command is pending drops the last reference to the killed dev->non_ordered, and percpu_ref_put() then runs target_non_ordered_release() in the completing context. Both take the lock and, if commands are waiting, call schedule_work(&dev->delayed_cmd_work), which queues on system_percpu_wq, i.e. on the CPU that took the completion. Further completions for the same queue are typically delivered there too, so one arriving while the work holds the lock spins on it forever. Reaching this needs complete_type=1, which is not the default (vhost-scsi, the only fabric with direct_compl_supp, defaults to TARGET_QUEUE_COMPL), a backend whose I/O completes from interrupt context, and ORDERED commands from the initiator. Linux virtio_scsi guests send only VIRTIO_SCSI_S_SIMPLE and never take the ordered path; any guest that uses the ORDERED task attribute, which vhost-scsi accepts, does. target_do_delayed_work() is a work item and always runs in process context, so spin_lock_irq() is sufficient. Found by inspection; no runtime report. A single ORDERED command goes through both acquisitions, so with CONFIG_PROVE_LOCKING the first one completed through direct completion should produce an inconsistent lock state report on delayed_cmd_lock (hardirq or softirq, depending on where the backend completes).	N/A	More Deta
CVE-2026-99208	In the Linux kernel, the following vulnerability has been resolved: drm/xe/oa: Zero OA buffer at allocation ttm_bo_type_kernel BOs are not guaranteed to be zeroed on allocation and may contain data from previously freed pages. Since the OA buffer is mmap'able by userspace, this can expose stale kernel memory contents. Streams opened with DRM_XE_OA_PROPERTY_OA_DISABLED allocate the OA buffer without calling xe_oa_init_oa_buffer(). Zero the buffer at allocation to prevent information disclosure through mmap. The existing zeroing in xe_oa_init_oa_buffer() remains necessary for zero report-id/timestamp detection on enable/re-enable. (cherry picked from commit 126c4c5388f9311a390b9b254a835b0cf0f55331)	N/A	More Deta
CVE-2026-99209	In the Linux kernel, the following vulnerability has been resolved: drm/xe: skip eviction of a BO with no resource xe_evict_flags() switches on tbo->resource->mem_type to choose an eviction placement. An xe BO can reach eviction with no ttm.resource, e.g. an imported dma-buf BO whose resource was freed during teardown while its attachment is still live: the exporter then invalidates it via xe_dma_buf_move_notify() -> xe_bo_evict(), and the switch dereferences a NULL resource and faults. A BO with no resource has nothing placed or mapped, so there is nothing to evict. Return an empty placement (num_placement = 0), mirroring the handling already used for non-xe scatter-gather BOs just above; ttm_bo_validate() then takes the pipeline-gutting path and returns 0. Without the fix the xe_dma_buf@xe_test_dmabuf_move_notify_no_resource dynamic live selftest will fail with below stack. BUG: kernel NULL pointer dereference, address: 0000000000000010 RIP: 0010:xe_evict_flags+0xf4/0x140 [xe] Call Trace: <TASK> xe_bo_evict+0x40/0xa0 [xe] ? ttm_bo_pipeline_gutting+0x71/0x180 [ttm] xe_test_dmabuf_move_notify_no_resource+0x182/0x440 [xe] xe_dma_buf_kunit+0x387/0x580 [xe] v2: Add Fixes tag and failure info in commit text (Matt Brost) (cherry picked from commit dbcfaac6331f1fcb0c2fe3ad3e9adb1e5d43ec0c)	N/A	More Deta
CVE-2026-99210	In the Linux kernel, the following vulnerability has been resolved: accel/rocket: clear rdev on device init failure rocket_probe() stores the return value from rocket_device_init() in the file-scoped rdev pointer before checking whether it is an error pointer. If rocket_device_init() fails, rdev is left as an ERR_PTR. The rdev pointer is also used as the marker for whether the shared rocket device has already been initialized. A later core probe can therefore see a non-NULL rdev, skip rocket_device_init(), and dereference the error pointer when reading rdev->num_cores. Save the error code and clear rdev before returning from the rocket_device_init() failure path.	N/A	More Deta
CVE-2026-99211	In the Linux kernel, the following vulnerability has been resolved: netlink: reset skb headers before unicast and multicast filtering Socket filters can use SKF_NET_OFF and SKF_LL_OFF to read relative to an skb's network and MAC headers. Netlink producers may reserve headroom without resetting those headers, allowing a receiving socket's filter to read data before the initialized message. For example, IWPM HELLO replies are allocated with dev_alloc_skb(), which reserves NET_SKB_PAD bytes. An unprivileged NETLINK_RDMA user can attach a classic socket filter and disclose this headroom through the length of the delivered reply. The resets in netlink_dump() do not help because IWPM sends a separately allocated skb through netlink_unicast(). Reset both headers before running the receiver's filter in unicast and broadcast delivery, as is already done for dump skbs. This also covers other netlink producers that reserve headroom without changing their allocation or message-building code.	N/A	More Deta
CVE-2026-87100	Protection mechanism failure due to missing binary hardening in Linux executables. The following products are affected: Acronis Cyber Protect 17 (Linux) before build 42587.	N/A	More Deta
CVE-2026-99214	In the Linux kernel, the following vulnerability has been resolved: drm/vc4: hdmi: Move packet RAM enable to PM runtime Audio can be triggered by the HPD handler and start up before video has been restored, calling vc4_hdmi_write_infoframe() for the audio infoframe. vc4_hdmi_write_infoframe() needs Packet RAM to be on to store the infoframe, however, if the video hasn't been enabled, vc4_hdmi_encoder_post_crtc_enable() hasn't been called and therefore, the Packet RAM can be disabled by the time vc4_hdmi_write_infoframe() executes, causing the following splat: [201.570266] ------------[cut here]------------ [201.570293] Packet RAM has to be on to store the packet. [201.570367] WARNING: drivers/gpu/drm/vc4/vc4_hdmi.c:683 at vc4_hdmi_write_infoframe+0x404/0x494 [vc4], CPU#0: wireplumber/1606 [...] [201.658650] Hardware name: Raspberry Pi 4 Model B Rev 1.5 (DT) [...] [201.758499] Call trace: [201.760967] vc4_hdmi_write_infoframe+0x404/0x494 [vc4] (P) [201.766607] vc4_hdmi_write_audio_infoframe+0x1c/0x28 [vc4] [201.772247] write_infoframe+0xbc/0x140 [drm_display_helper] [201.777975] drm_atomic_helper_connector_hdmi_update_audio_infoframe+0x80/0xdc [drm_display_helper] [201.787140] vc4_hdmi_audio_prepare+0x4ac/0x570 [vc4] [201.792252] drm_connector_hdmi_audio_prepare+0x24/0x30 [drm_display_helper] [201.799390] hdmi_codec_prepare+0x100/0x160 [snd_soc_hdmi_codec] [201.805471] snd_soc_pcm_dai_prepare+0xd4/0x100 [snd_soc_core] [201.811375] __soc_pcm_prepare+0x60/0x12c [snd_soc_core] [201.816752] soc_pcm_prepare+0x34/0x58 [snd_soc_core] [201.821863] snd_pcm_do_prepare+0x70/0x8c [snd_pcm] [201.826798] snd_pcm_action_nonatomic+0xe4/0x174 [snd_pcm] [201.832350] snd_pcm_prepare+0xc8/0xd8 [snd_pcm] [201.837021] snd_pcm_common_ioctl+0x458/0x614 [snd_pcm] [201.842308] snd_pcm_ioctl+0x30/0x48 [snd_pcm] [201.846802] __arm64_sys_ioctl+0x88/0xd8 [201.850769] invoke_syscall+0x48/0xf4 [201.854470] el0_svc_common+0x80/0xd8 [201.858171] do_el0_svc+0x1c/0x28 [201.861520] el0_svc+0x3c/0xb0 [201.864605] el0t_64_sync_handler+0x68/0xdc [201.868834] el0t_64_sync+0x198/0x19c [201.872536] ---[end trace 0000000000000000]--- Considering that Packet RAM enable is essentially a power management configuration, move its enabling/disabling to the Runtime PM hooks. Note that post_crtc_disable() still stops all infoframes, but keeps Packet RAM enabled, leaving it to be disabled by runtime suspend.	N/A	More Deta
	In the Linux kernel, the following vulnerability has been resolved: power: supply: core: prevent unregistering a power supply while a callback runs		

CVE-2026-99215	Once a power supply is registered, its callbacks can immediately start firing from other contexts, such as external_power_changed() triggered by the TCPM stack. If a power supply is unregistered while the callback is still running, the driver data can already be freed when the callback tries to access it, leading to a use-after-free. This happens e.g. when the hardware bus carrying the power supply device malfunctions (e.g. I2C is hogged down by another malfunctioning device) immediately after the power supply is registered, and thus the core is still processing the callbacks which were queued up when the driver starts the removal, leading in some cases to a kernel crash, e.g.: [11.645942] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000005 [11.646751] Mem abort info: [11.647006] ESR = 0x0000000096000004 [11.647338] EC = 0x25: DABT (current EL), IL = 32 bits [11.647806] SET = 0, FnV = 0 [11.648077] EA = 0, S1PTW = 0 [11.648356] FSC = 0x04: level 0 translation fault [11.648785] Data abort info: [11.649041] ISV = 0, ISS = 0x00000004, ISS2 = 0x00000000 [11.649524] CM = 0, WnR = 0, TnD = 0, TagAccess = 0 [11.649981] GCS = 0, Overlay = 0, DirtyBit = 0 [11.650390] [0000000000000005] user address but active_mm is swapper [11.650955] Internal error: Oops: 0000000096000004 [#1] SMP [11.651460] Modules linked in: [11.651742] CPU: 1 UID: 0 PID: 144 Comm: kworker/1:2 Not tainted 7.2.0-rc6-g62a9297af2cd #1 PREEMPT [11.652553] Hardware name: Flipper One rev. F0B1C2 (DT) [11.653024] Workqueue: events power_supply_changed_work [11.653511] pstate: 60000005 (nZCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) [11.654135] pc : __power_supply_is_supplied_by+0x18/0x100 [11.654624] lr : __power_supply_am_i_supplied+0x40/0xb8 [11.655098] sp : ffff80008192bb30 [11.655399] x29: ffff80008192bb30 x28: 0000000000000000 x27: 0000000000000000 [11.656049] x26: 0000000000000000 x25: 0000000000000000 x24: 0000000000000000 [11.656695] x23: ffff0000c19f4200 x22: ffffdb2232ba4ea8 x21: ffff80008192bc28 [11.657344] x20: ffff0000c1eef000 x19: ffff80008192bc18 x18: 00000000a0886e62 [11.657991] x17: 000000040044ffff x16: 04500072b5503510 x15: 0000000000000000 [11.658639] x14: 0000000000000000 x13: 0000000000000220 x12: 0000000000000000 [11.659286] x11: 0000000000000000 x10: ffff0000c1fdb2b0 x9 : ffffdb2232ba5590 [11.659934] x8 : 00000000e5b906e6 x7 : ffff0000c2502778 x6 : ffffdb22339793d0 [11.660581] x5 : ffff80008192bc18 x4 : ffff0000c19cbca0 x3 : 0000000000000000 [11.661228] x2 : ffff0000c1fdaf40 x1 : fffffffffffffed x0 : ffff0000c1eef000 [11.661878] Call trace: [11.662103] __power_supply_is_supplied_by+0x18/0x100 (P) [11.662596] __power_supply_am_i_supplied+0x40/0xb8 [11.663040] psy_for_each_psy_cb+0x20/0x40 [11.663416] class_for_each_device+0x110/0x150 [11.663825] power_supply_am_i_supplied+0x68/0x100 [11.664262] bq257xx_external_power_changed+0x58/0x140 [11.664733] __power_supply_changed_work+0x60/0x80 [11.665170] psy_for_each_psy_cb+0x20/0x40 [11.665545] class_for_each_device+0x110/0x150 [11.665953] power_supply_changed_work+0x98/0x1b8 [11.666382] process_one_work+0x164/0x4c0 [11.666758] worker_thread+0x19c/0x320 [11.667104] kthread+0x138/0x150 [11.667408] ret_from_fork+0x10/0x20 [11.667744] Code: d503233f a9bd7bfd 910003fd a90153f3 (f9400c34) [11.668294] ---[end trace 0000000000000000]--- Add a read-write semaphore between external_power_changed() and power_supply_unregister() to prevent the latter from returning (and thus the driver from freeing its data) while the callback is still running.	N/A	More Deta
CVE-2026-118668	langgraph-api implements the LangGraph API for rapid development and testing. From 0.1.2 until 0.15.0, JavaScript or TypeScript custom authentication Store authorization handlers can return a rewritten namespace that is not carried across the runtime boundary and applied before the Store operation. An authenticated user can therefore access another user's Store namespace when a deployment relies on namespace rewriting for isolation, allowing unauthorized reads, overwrites, searches, or deletions. Python custom authentication and handlers that reject unauthorized namespaces instead of rewriting them are not affected. This issue is fixed in version 0.15.0.	N/A	More Deta
CVE-2026-117790	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-118551	Insecure Storage of Sensitive Information vulnerability in Drupal AI (Artificial Intelligence) allows Retrieve Embedded Sensitive Data. This issue affects AI (Artificial Intelligence) versions: from 0.0.0 to 1.4.11, from 1.5.0 to 1.5.2.	N/A	More Deta
CVE-2026-117718	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-112197	Vulnerability due to a lack of authentication in critical functions of the NoviGest Desktop App's Java RMI service. An attacker with network access to the service can invoke remote methods without authentication, obtain sensitive credentials, and execute arbitrary SQL queries on PostgreSQL. The elevated privileges of the database account allow these capabilities to be chained together to execute operating system commands on the server, compromising its confidentiality, integrity, and availability.	N/A	More Deta
CVE-2026-118764	minimatch is a minimal matching utility for converting glob expressions into JavaScript RegExp objects. Starting in 7.0.0 and prior to 11.0.1, src/index.ts implements firstPhasePreProcess() so that, at optimizationLevel 2 or higher, it repeatedly expands attacker-controlled **/.. pattern segments inside a fixpoint loop, allowing generated globParts entries to be processed and expanded again. secondPhasePreProcess() then compares the expanded entries pairwise, so a short malicious glob can cause excessive CPU and memory consumption during pattern compilation. This issue is fixed in version 11.0.1.	N/A	More Deta
CVE-2026-118765	Botan is a C++ cryptography library. From 3.7.0 until 3.13.0, an application that calls AutoSeeded_RNG::clear() and then calls randomize with an empty output buffer while the generator is unseeded can cause AutoSeeded_RNG to mark itself seeded without consulting the configured entropy source. On builds without BOTAN_HAS_SYSTEM_RNG, the fallback uses only a clock value and process ID, so a later non-empty request can produce output from predictable state. This issue is fixed in version 3.13.0.	N/A	More Deta
CVE-2026-62374	SD JWT JS is a JavaScript implementation of the Selective Disclosure JWT (SD-JWT) specification. In version 0.19.0 and earlier, `@sd-jwt/decode`, also used by `@sd-jwt/core`, silently drops a tampered Disclosure whose digest no longer matches the Issuer-signed `_sd` array and returns a reduced claim set, reporting success while the Issuer signature remains valid. Both a tampered Disclosure that remains valid JSON and a Disclosure containing invalid UTF-8 bytes reach this silent-drop behavior. In the latter case, the `TextDecoder / Buffer` decoding path substitutes U+FFFD replacement characters, recovering syntactically valid disclosure data instead of rejecting the malformed input. This violates RFC 9901 section 7.1 step 5, which requires rejection of unreferenced Disclosures, and section 7.1 step 3 / section 4.2.1, which require rejection of invalid Disclosures. A malicious holder can exploit this omission primitive, including through `SDJwtInstance.verify()` when key binding is required. An on-path attacker can also tamper with a Disclosure when the relying party does not enforce key binding; enforced key binding rejects on-path tampering because it invalidates the KB-JWT `sd_hash` binding. If the relying party defaults to allowing access when a constraining age, role, or restriction claim is absent, the silent claim reduction can change an authorization decision without an error. This issue is fixed in `@sd-jwt/core` version 0.20.0; no patched version of the standalone `@sd-jwt/decode` package is identified.	N/A	More Deta
CVE-2026-116566	socket.getaddrinfo() previously accepted null bytes within *host* and *port* parameters which can cause the values to be silently truncated.	N/A	More Deta
CVE-2026-118768	Botan is a C++ cryptography library. From 1.11.34 until 3.13.0, the botan ocsp_check command requested an OCSP response from a certificate's Authority Information Access URL without verifying the response signature or authorizing the signer. A malicious responder or on-path attacker could return a matching and timely GOOD response with an empty, invalid, or unauthorized signature, causing a revoked certificate to produce exit status 0 and OCSP check OK output. Only the command-line interface is affected. This issue is fixed in version 3.13.0.	N/A	More Deta
CVE-2026-118769	Botan is a C++ cryptography library. From 2.1.0 until 3.13.0, the Botan C API function botan_block_cipher_block_size converted a size_t block size to int without a bounds check. In an application that accepts external algorithm parameter strings and uses the FFI raw ECB mode, an attacker can select the variable-block-size Lion cipher so that the reported size is truncated, the caller allocates insufficient memory, and later block processing	N/A	More Deta

	causes memory corruption. The C++ API and normally used C API modes such as CBC and CTR are unaffected. This issue is fixed in version 3.13.0.		
CVE-2026-60111	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Deta
CVE-2026-103093	ServiceNow has remediated a sandbox escape security issue that was identified in the ServiceNow AI Platform. This vulnerability could enable an authenticated user with the admin role to bypass Rhino sandbox restrictions and execute arbitrary code on the underlying host operating system, potentially enabling further unintended access. ServiceNow deployed an update to hosted instances, and ServiceNow provided the update to our partners and self-hosted customers. We are not currently aware of malicious exploitation against ServiceNow instances. We recommend customers promptly apply appropriate updates or upgrade to a patched release if they have not already done so.	N/A	More Deta
CVE-2026-103094	ServiceNow has remediated an information disclosure vulnerability that was identified in the ServiceNow AI Platform. This vulnerability could cause a user's plaintext password to be persisted in a system table, potentially exposing that password to a user who otherwise would not be entitled to view it. ServiceNow remediated the vulnerability through security updates that address the unintended persistence of plaintext credentials. We are not currently aware of malicious exploitation against ServiceNow instances. We recommend customers promptly apply appropriate updates or upgrade to a patched release if they have not already done so.	N/A	More Deta
CVE-2026-101274	When pretix is used as the identity provider in a Single-Sign-On (SSO) setup for customer accounts, the system did not properly validate the `response_type` requested in an authorization request against the configured grant type of the SSO client. This means that if an SSO client was configured to only allow the `code` response type, which requires knowledge of the client secret to use and would wrongfully send a response type like `id_token`, it would receive back a valid token. Exploiting this requires the attacker to run JavaScript on the page specified by `redirect_uri`, which must be from a list specified in the client configuration.	N/A	More Deta
CVE-2026-118773	Glob matches files using patterns the shell uses. From 9.0.0 until 14.0.2, abort branches in src/walker.ts, including GlobUtil.walkCB(), GlobUtil.walkCB2(), GlobUtil.walkCBSync(), and GlobUtil.walkCB2Sync(), invoke the callbacks without returning. After AbortSignal or AbortSignal.timeout() rejects or emits an error, execution can continue into processor.processPatterns(), readdirCB(), and recursive traversal. The issue affects glob() and globStream() when applications expose attacker-influenced patterns or directory trees and rely on cancellation as a traversal budget. Repeated timed-out requests can stack background filesystem operations and CPU work, degrading worker throughput or service availability; no confidentiality or integrity impact was observed. This issue is fixed in 14.0.2.	N/A	More Deta
CVE-2026-101273	Some of our API endpoints allowed to create order payments referencing a gift card by using the auto-incremented internal ID. This ID was not checked and allowed creating payments that reference gift cards from different organizers and thereby obtaining their secret. The gift card is not charged in this case, but by then triggering a refund on the payment, one can increase the value of the gift card.	N/A	More Deta
CVE-2026-101272	The mechanism binding files generated during a shredding process to the authentication method is not working correctly and the same session token is used for all token-based API users. This is similar to an issue fixed in 2026.7.1 but was missed while creating the fix. Since the files are referred to by randomly generated UUIDs and only exist for a day, there is virtually no risk, but it renders the added protection mechanism useless. As part of the fix, we have also improved hardening of some other related code areas.	N/A	More Deta
CVE-2025-30414	Local privilege escalation due to improper authentication. The following products are affected: Acronis Cyber Protect Cloud Agent (Windows) before build 42569, Acronis Cyber Protect 17 (Windows) before build 42587.	N/A	More Deta
CVE-2026-58118	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Deta
CVE-2026-58119	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Deta
CVE-2026-58120	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Deta
CVE-2026-6877	ServiceNow has addressed a domain separation bypass security issue that was identified in the ServiceNow SR – CSM – Task Plan Templates Store application. This vulnerability could enable an authenticated user with a specific role to create records in domains they do not have access to, potentially leading to unauthorized data creation across domain boundaries. We are not currently aware of malicious exploitation against ServiceNow instances. We recommend customers promptly apply appropriate updates or upgrade to a patched release if they have not already done so.	N/A	More Deta
CVE-2026-119193	PHPUnit is a testing framework for PHP. From 13.4.0 until 13.4.4, the TestCase::coverageFilesDirectory() logic in src/Runner/Phpt/TestCase.php creates temporary files for PHPT code coverage in a predictable phpunit-phpt directory under sys_get_temp_dir() and reuses that directory without verifying its ownership or permissions. On multi-user systems with a shared temporary path, a local attacker who creates the directory before the developer runs PHPT tests with code coverage can replace the generated job file before the child process executes it with require, allowing arbitrary code execution with the developer's privileges while the test and coverage report appear successful. PHPUnit 12.5 and earlier, default macOS and Windows configurations with per-user temporary directories, and single-user environments where another user cannot create files in the temporary path are not affected. This issue is fixed in 13.4.4.	N/A	More Deta
CVE-2026-14571	A Blind SQL Injection vulnerability in Futurum Software’s management software, caused by a lack of adequate validation and sanitisation of user-provided inputs in queries to the private area’s database, as well as by an incorrect WAF configuration. This weakness allows the protection mechanisms to be bypassed solely by sending manipulated HTTP requests. Successful exploitation of the vulnerability could allow an unauthenticated attacker to execute arbitrary queries against the database, extract its complete structure and gain access to sensitive customer information, including personally identifiable information (PII).	N/A	More Deta
CVE-2026-67203	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Deta
CVE-2026-67205	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Deta
	Lightdash is an open source business intelligence platform. In affected versions through 0.3213.0, the dbt Cloud webhook `POST /api/v1/projects/{projectUuid}/dbt-cloud/webhook` has no authentication middleware or signature validation. In `packages/backend/src/controllers/projectController.ts`, `testWebhook()` accepts `accountId` and `runId` from a `job.run.completed` request and		

CVE-2026-61576	passes them to `createPreviewWithExplores()` in `packages/backend/src/services/ProjectService/ProjectService.ts`. These unsanitized values are interpolated into the server-side dbt Cloud API URL, which is requested with the victim project's API key in the `Authorization` header. Path traversal through `accountId` changes the requested path on `cloud.getdbt.com` without changing its host, so the credential-bearing request reaches an attacker-influenced path on that fixed host. The advisory claims API-key theft, but the supplied evidence does not establish that the attacker can observe the `Authorization` header. The unauthenticated webhook also allows preview creation. The target must be a `dbt Cloud IDE` project and the attacker must know its `projectUuid`; the UUID is not enumerable but can be discovered in shared or multi-tenant contexts. Version 0.3214.0 fixes identifier path traversal and verifies webhook HMAC signatures only when a secret is configured; without a secret, unsigned webhooks continue to be processed.	N/A	More Deta
CVE-2026-115943	Spreadsheet::XLSX versions before 0.19 for Perl allow code execution via string eval of number format conditions in ExcelFmt. When a number format has a condition such as [>100], ExcelFmt chooses the format section by passing the condition and the cell value to a string eval. Both come from the workbook, and the eval runs while Spreadsheet::XLSX->new parses it. An attacker who supplies an XLSX file can run arbitrary Perl code.	N/A	More Deta
CVE-2026-119282	Nx is a monorepo solution for TypeScript and polyglot codebases. From 22.0.2 until 22.7.9 and 23.1.2 for @nx/maven, and from 21.0.0 until 22.7.9 and 23.1.2 for @nx/gradle, the plugins' project-graph analyzers launch through a shell and interpolate plugin options from nx.json into command arguments. The @nx/maven targetNamePrefix value and arbitrary @nx/gradle option names or values can therefore be interpreted as shell syntax whenever an nx command constructs the project graph. A user who runs Nx in an attacker-controlled repository or pull request can execute injected commands with the user's privileges, while workspaces that register neither affected plugin are not exposed to this path. Remediation requires upgrading both nx and each affected plugin to matching releases because the plugin fix depends on code in the nx package. This issue is fixed in versions 22.7.9 and 23.1.2.	N/A	More Deta
CVE-2026-119284	joserfc is a Python library that provides an implementation of several JSON Object Signing and Encryption (JOSE) standards. Prior to 1.7.6, joserfc compact JWS deserialization calls bytes.split() before enforcing the existing aggregate segment-size limits. When attacker-controlled compact serialization bytes reach deserialize_compact(), the split creates copies of the header, payload, and signature segments before ExceededSizeError rejects them, causing an additional allocation approximately proportional to the supplied token. Requests that exhaust available process memory can therefore cause an availability failure even though signature verification fails. This issue is fixed in version 1.7.6.	N/A	More Deta
CVE-2026-61654	Lightdash is an open source business intelligence platform. In affected versions through 0.3213.0, the dbt Cloud webhook `POST /api/v1/projects/{projectUuid}/dbt-cloud/webhook` has no authentication middleware or signature validation. In `packages/backend/src/controllers/projectController.ts`, `testWebhook()` accepts `accountId` and `runId` from a `job.run.completed` request and passes them to `createPreviewWithExplores()` in `packages/backend/src/services/ProjectService/ProjectService.ts`. These unsanitized values are interpolated into the server-side dbt Cloud API URL, which is requested with the victim project's API key in the `Authorization` header. Path traversal through `accountId` changes the requested path on `cloud.getdbt.com` without changing its host, so the credential-bearing request reaches an attacker-influenced path on that fixed host. The advisory claims API-key theft, but the supplied evidence does not establish that the attacker can observe the `Authorization` header. The unauthenticated webhook also allows preview creation. The target must be a `dbt Cloud IDE` project and the attacker must know its `projectUuid`; the UUID is not enumerable but can be discovered in shared or multi-tenant contexts. Version 0.3214.0 fixes identifier path traversal and verifies webhook HMAC signatures only when a secret is configured; without a secret, unsigned webhooks continue to be processed.	N/A	More Deta
CVE-2026-61673	WeGIA is a web manager for charitable institutions. Prior to 3.8.7, a stored DOM cross-site scripting vulnerability in `web/html/memorando/listar_despachos.php` results from unsafe handling of the `texto` field. The affected flow spans `web/controle/memorando/DespachoControle.php` and `web/dao/memorando/DespachoDAO.php`: `FILTER_SANITIZE_SPECIAL_CHARS` is applied during storage, but `html_entity_decode()` later decodes the stored content and `jQuery .html()` inserts the result into the DOM. An attacker able to submit a memorandum dispatch through `/controle/control.php` using `DespachoControle` and `metodo=incluir` can store malicious HTML or JavaScript. The code executes automatically when another user views the memorandum thread through `/html/memorando/listar_despachos.php` with `id_memorando`. This permits arbitrary JavaScript execution, theft of administrator `PHPSESSID` session tokens, privileged session hijacking, account takeover, and unauthorized access to privileged or internal functionality. This issue is fixed in version 3.8.7.	N/A	More Deta
CVE-2026-112198	XML External Entity (XXE) injection vulnerability in the SAFT import feature of the NoviGest Desktop App. The application processes user-controlled XML files using a JAXB Unmarshaller without properly disabling external entity resolution. An attacker with access to this functionality could provide a manipulated XML file to read local files accessible to the application process. If the application runs with elevated privileges, sensitive system files could be exposed.	N/A	More Deta
CVE-2026-117692	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117693	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117706	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-118673	KeePassXC is a cross-platform community-driven port of the Windows application KeePass Password Safe. From 2.3.0 until 2.8.0, KeePassXC browser integration encrypts authorized responses in src/browser/BrowserMessageBuilder.cpp using a fixed 1 MiB output vector even though Botan::Sodium::crypto_box_easy() writes the plaintext length plus crypto_box_MACBYTES. A browser-protocol client that can access the per-user IPC endpoint, has a valid database association, and causes an unlocked database to generate and encrypt a sufficiently large authorized response can trigger a sequential out-of-bounds write before any response is delivered. This issue is fixed in version 2.8.0.	N/A	More Deta
CVE-2026-117716	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117715	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117714	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta

117713			
CVE-2026-117712	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117711	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-66911	Zimbra is vulnerable to stored cross-site scripting (XSS) via the Content-Location MIME header in email attachments. Due to lack of sanitization of the Content-Location header, an attacker can set it to a javascript: URI. An unauthenticated remote attacker can send a crafted email to a victim; when the victim opens the email in the Zimbra web interface and clicks the attachment name, the JavaScript payload executes in the victim's browser context. This issue was fixed in version 10.1.21	N/A	More Deta
CVE-2026-66912	Zimbra is vulnerable to Stored Cross-Site Scripting (XSS) via the From email header during HTML reply composition in Classic UI. Due to insufficient sanitization of the From header value, a remote attacker can send a crafted email containing a malicious From header with an embedded JavaScript payload. When the victim opens the message in Classic UI and clicks Reply while composing in HTML mode with reply headers disabled, the unsanitized From header content is rendered as HTML and the JavaScript payload executes in the victim's browser, potentially allowing the attacker to steal session information or perform actions on behalf of the victim. This issue was fixed in version 10.1.21	N/A	More Deta
CVE-2026-117710	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117709	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117708	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117707	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117705	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117694	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117704	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-93570	Szafir and Szafir Weryfikująca are vulnerable to XML External Entity (XXE) injection. When a user signs or verify a crafted XML file containing a `DOCTYPE` with an external DTD reference, the parser processes external entities, allowing an attacker to read arbitrary files from the victim's filesystem. This issue was fixed in Szafir version 2.0 build 708. Szafir Weryfikująca is no longer supported (End of Life) and has not been fixed.	N/A	More Deta
CVE-2026-99113	In the Linux kernel, the following vulnerability has been resolved: ksmbd: zero the FS_OBJECT_ID_INFORMATION buffer before filling it in smb2_get_info_filesystem() reports 64 bytes for FS_OBJECT_ID_INFORMATION, that is the whole of struct object_id_info, but writes only 46 of them: - objid[] is 16 bytes, and when the volume UUID is not available only sizeof(stfs.f_fsid) (8) bytes are copied into it; - extended_info.version_string[] is STRING_LENGTH (28) bytes, and only strlen("1.1.0") (5) bytes are copied into it. The response buffer is zeroed on allocation (kvzalloc() in smb2_allocate_rsp_buf()), so for a standalone request the remaining 31 bytes are zero. In a compound request they need not be. The offset of the next response is advanced by the length pinned for the previous one, so if a preceding command wrote its reply into the buffer and then failed, smb2_set_err_rsp() pins only the short error response and the next reply lands inside the area that has already been written. Only the header is cleared there: memset((char *)rsp_hdr, 0, sizeof(struct smb2_hdr) + 2); The client then receives up to 31 bytes of a response it was not meant to see, including one that failed with an access denied error. Clear the structure before filling it in. As a side effect version_string is now NUL terminated.	N/A	More Deta
CVE-2026-117703	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117702	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117701	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117700	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117699	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2023-7357	A remote code execution (RCE) vulnerability was identified in the FlexNet Publisher lmadmin web user interface. This vulnerability is addressed in the FlexNet Publisher 2023 R2 (11.19.4.0) release.	N/A	More Deta

CVE-2026-117698	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117697	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117696	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117695	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2023-22793	A vulnerability allowing an unauthenticated attacker to perform remote code execution (RCE) on servers running the Veeam Virtualization Extensions service of Veeam Management Pack for Microsoft System Center.	N/A	More Deta
CVE-2026-107238	A vulnerability allowing an authenticated domain user to perform remote code execution (RCE) as the LocalSystem account on servers running the Veeam Management Pack for Microsoft System Center Collector service.	N/A	More Deta
CVE-2026-107239	A vulnerability allowing a member of the Veeam Virtualization Extensions Users group to perform remote code execution (RCE) on servers running the Veeam Management Pack for Microsoft System Center Collector service.	N/A	More Deta
CVE-2026-114548	Use of Web Browser Cache Containing Sensitive Information vulnerability in Drupal ImageAPI Optimize WebP allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects ImageAPI Optimize WebP versions: from 0.0.0 to 2.1.2.	N/A	More Deta
CVE-2026-114535	Missing Authorization vulnerability in Drupal Swiper formatter allows Forceful Browsing. This issue affects Swiper formatter versions: from 0.0.0 to 2.1.2, from 3.0.1 to 3.1.0.	N/A	More Deta
CVE-2026-114536	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal USWDS Paragraph Components allows Stored XSS. This issue affects USWDS Paragraph Components versions: from 0.0.0 to 3.1.3.	N/A	More Deta
CVE-2026-114537	Incorrect Authorization vulnerability in Drupal View Unpublished allows Forceful Browsing. This issue affects View Unpublished versions: from 0.0.0 to 1.5.0.	N/A	More Deta
CVE-2026-114538	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Bootstrap allows Cross-Site Scripting (XSS). This issue affects Bootstrap versions: from 0.0.0 to 3.45.0.	N/A	More Deta
CVE-2026-114539	Authentication Bypass Using an Alternate Path or Channel vulnerability in Drupal DocCheck Basic allows Authentication Bypass. This issue affects DocCheck Basic versions: 7.x.	N/A	More Deta
CVE-2026-114540	Incorrect Authorization vulnerability in Drupal Domain allows Forceful Browsing. This issue affects Domain versions: from 3.0.0 to 3.0.2.	N/A	More Deta
CVE-2026-114541	Cross-Site Request Forgery (CSRF) vulnerability in Drupal Frontend Editing allows Cross Site Request Forgery. This issue affects Frontend Editing versions: from 0.0.0 to 1.9.3.	N/A	More Deta
CVE-2026-114542	Use of Web Browser Cache Containing Sensitive Information vulnerability in Drupal Simple OAuth (OAuth2) & OpenID Connect allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Simple OAuth (OAuth2) & OpenID Connect versions: from 6.1.0 to 6.1.3.	N/A	More Deta
CVE-2026-114543	Incorrect Authorization vulnerability in Drupal Simple User Management allows Forceful Browsing. This issue affects Simple User Management versions: from 0.0.0 to 1.11.0.	N/A	More Deta
CVE-2026-114544	Incorrect Authorization vulnerability in Drupal Media Bulk Upload allows Forceful Browsing. This issue affects Media Bulk Upload versions: from 0.0.0 to 3.0.6.	N/A	More Deta
CVE-2026-114545	Incorrect Authorization vulnerability in Drupal Fullcalendar View allows Forceful Browsing. This issue affects Fullcalendar View versions: from 0.0.0 to 5.2.6.	N/A	More Deta
CVE-2026-114546	Use of Web Browser Cache Containing Sensitive Information vulnerability in Drupal Media Alias Display allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Media Alias Display versions: from 0.0.0 to 2.1.2, from 3.0.0 to 3.0.2.	N/A	More Deta
CVE-2026-114547	Missing Authorization vulnerability in Drupal TinyPNG allows Forceful Browsing. This issue affects TinyPNG versions: from 0.0.0 to 2.0.2.	N/A	More Deta
CVE-2026-114553	Incorrect Authorization vulnerability in Drupal Frontend Editing allows Forceful Browsing. This issue affects Frontend Editing versions: from 0.0.0 to 1.9.3.	N/A	More Deta
CVE-			

2026-114533	Missing Authorization vulnerability in Drupal Ágora Transparency Theme allows Forceful Browsing. This issue affects Ágora Transparency Theme versions: from 0.0.0 to 1.2.3.	N/A	More Deta
CVE-2026-114554	Incorrect Authorization vulnerability in Drupal AI File to Text allows Forceful Browsing. This issue affects AI File to Text versions: from 0.0.0 to 1.0.1.	N/A	More Deta
CVE-2026-114571	Incorrect Authorization vulnerability in Drupal Rabbit Hole allows Forceful Browsing. This issue affects Rabbit Hole versions: from 0.0.0 to 1.3.0.	N/A	More Deta
CVE-2026-114573	Improperly Controlled Modification of Dynamically-Determined Object Attributes vulnerability in Drupal Monster Menus allows Object Injection. This issue affects Monster Menus versions: from 0.0.0 to 9.5.6.	N/A	More Deta
CVE-2026-118540	Incorrect Authorization vulnerability in Drupal Commerce Core allows Forceful Browsing. This issue affects Commerce Core versions: from 0.0.0 to 2.41, from 3.0.0 to 3.2.0.	N/A	More Deta
CVE-2026-118541	Incorrect Authorization vulnerability in Drupal Commerce Core allows Forceful Browsing. This issue affects Commerce Core versions: from 0.0.0 to 2.41.0, from 3.0.0 to 3.3.13.	N/A	More Deta
CVE-2026-118542	Incorrect Authorization vulnerability in Drupal Commerce Core allows Forceful Browsing. This issue affects Commerce Core versions: from 0.0.0 to 2.41.0, from 3.0.0 to 3.3.13.	N/A	More Deta
CVE-2026-118543	Cross-Site Request Forgery (CSRF) vulnerability in Drupal Commerce Core allows Cross Site Request Forgery. This issue affects Commerce Core versions: from 0.0.0 to 2.41.0, from 3.0.0 to 3.3.13.	N/A	More Deta
CVE-2026-118544	Exposure of Sensitive Information Through Data Queries vulnerability in Drupal Commerce Core allows Forceful Browsing. This issue affects Commerce Core versions: from 0.0.0 to 2.41.0, from 3.0.0 to 3.3.13.	N/A	More Deta
CVE-2026-118545	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal AI (Artificial Intelligence) allows Cross-Site Scripting (XSS). This issue affects AI (Artificial Intelligence) versions: from 0.0.0 to 1.4.11, from 1.5.0 to 1.5.2.	N/A	More Deta
CVE-2026-118546	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal AI (Artificial Intelligence) allows Cross-Site Scripting (XSS). This issue affects AI (Artificial Intelligence) versions: from 0.0.0 to 1.4.11, from 1.5.0 to 1.5.2.	N/A	More Deta
CVE-2026-118548	Incorrect Authorization vulnerability in Drupal AI (Artificial Intelligence) allows Resource Injection. This issue affects AI (Artificial Intelligence) versions: from 0.0.0 to 1.4.11, from 1.5.0 to 1.5.2.	N/A	More Deta
CVE-2026-118549	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal AI (Artificial Intelligence) allows Cross-Site Scripting (XSS). This issue affects AI (Artificial Intelligence) versions: from 0.0.0 to 1.4.11, from 1.5.0 to 1.5.2.	N/A	More Deta
CVE-2026-118550	Use of Web Browser Cache Containing Sensitive Information vulnerability in Drupal AI (Artificial Intelligence) allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects AI (Artificial Intelligence) versions: from 0.0.0 to 1.4.11, from 1.5.0 to 1.5.2.	N/A	More Deta
CVE-2026-114534	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Block Attributes allows Stored XSS. This issue affects Block Attributes versions: from 0.0.0 to 2.1.0.	N/A	More Deta
CVE-2026-114532	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal UI Icons allows Cross-Site Scripting (XSS). This issue affects UI Icons versions: from 0.0.0 to 1.1.3, from 2.0.0 to 2.0.2.	N/A	More Deta
CVE-2026-112211	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Deta
CVE-2026-107260	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Sector Distribution allows Stored XSS. This issue affects Sector Distribution versions: from 0.0.0 to 10.3.3, from 10.4.0 to 10.4.2.	N/A	More Deta
CVE-2026-92744	Under certain conditions, privilege manager agent allows a remote unauthenticated attacker to execute arbitrary code as LocalSystem.	N/A	More Deta
CVE-2026-112602	An authorization issue was addressed with improved state management. This issue is fixed in Xcode 27.2. An app may be able to access sensitive user data.	N/A	More Deta
CVE-2026-112605	This issue was addressed with improved handling of symlinks. This issue is fixed in Xcode 27.2. An app may be able to read arbitrary files.	N/A	More Deta
CVE-2026-15466	Software installed and run as a non-privileged user may conduct improper GPU system calls to cause race condition in hardware performance counters buffer’s destruction path leading to read and/or write UAF. The race condition in the destruction path could lead to reference counter being decremented in non-atomical way allowing other code paths using a freed object to read and/or write kernel heap memory.	N/A	More Deta
	A web page that contains unusual GPU shader code is loaded into the GPU compiler process and can lead memory allocation failure. If the		

CVE-2026-18629	allocation failure is not properly handled, the compiler may dereference a NULL pointer at a controlled offset, resulting in a crash of the compiler process. On certain platforms, when the compiler process has system privileges this could lead to crashes or enable further exploits on the device. The weakness results from performing arithmetic operations on values derived from the shader program without properly preventing integer overflow. The overflow can cause incorrect memory size calculations, leading to memory allocation failures and subsequent invalid program behaviour. Integer overflow can produce unexpected values that affect memory allocation and other security-relevant operations.	N/A	More Deta
CVE-2026-19199	Software installed and run as a non-privileged user may conduct improper system calls to allocate physical memory. A 32-bit integer overflow in the KM driver during page-to-byte conversion of an allocation size can result in an undersized kernel buffer allocation. This may allow unallocated or previously allocated physical pages to be mapped into an attacker-controlled GPU MMU context, leading to disclosure of sensitive kernel data.	N/A	More Deta
CVE-2026-65584	Software installed and run as a non-privileged user may conduct improper GPU system calls causing a stack overflow in the kernel. The overflow occurs when processing resolved Linux/Android fence synchronization checkpoints, while user checkpoints are excluded from the stack array. Successful exploitation can cause kernel memory corruption and typically results in a denial-of-service condition through a kernel crash. The code vulnerability is a buffer write beyond the allocated array on the stack caused by copying excessive data from an internal buffer.	N/A	More Deta
CVE-2026-65586	Software installed and run as a non-privileged user may conduct improper GPU system calls to free memory in still in use, replace with another allocation and cause arbitrary memory reads or writes to physical memory pages. A memory buffer managed by a CPU thread of control (driver) and accessed by a GPU thread of control (firmware) can be freed while in use. Software installed and run as a non-privileged user may replace that buffer with another and replace a shared resource (memory page address list) managed by the CPU thread of control (driver) leading to the GPU accessing memory not managed by the CPU thread of control (driver).	N/A	More Deta
CVE-2026-65587	A web page that contains unusual WebGPU content loaded into the GPU GLES render process can trigger an OOB write in the GPU user-space driver, leading to memory corruption and possible browser/GPU process crash. The software writes data past the end of an intended memory offset. Writing outside the bounds of allocated memory can corrupt adjacent memory, crash the process, or cause undefined behaviour.	N/A	More Deta
CVE-2026-74912	On GPU systems with the security vulnerability fix for CVE-2026-49746 applied, the mapping range of graphics buffers is limited which causes errors when the mapping outside of that range. Integer truncation caused when mapping GPU buffer pages in the buffer’s range 0GB - 4GB, produces error and limits the functionality of the kernel mode driver.	N/A	More Deta
CVE-2026-74915	A web page that contains unusual WebGPU content loaded into the GPU GLES render process can trigger a OOB read and/or write crash in the GPU GLES user-space shared library. On certain platforms, when the process executing graphics workload has system privileges this could enable further exploits on the device.	N/A	More Deta
CVE-2026-107255	Incorrect Authorization vulnerability in Drupal Restrict route by IP allows Forceful Browsing. This issue affects Restrict route by IP versions: from 0.0.0 to 1.3.1, from 2.0.0 to 2.0.1.	N/A	More Deta
CVE-2026-107256	Improper Restriction of Excessive Authentication Attempts vulnerability in Drupal Shield allows Brute Force. This issue affects Shield versions: from 0.0.0 to 1.9.0.	N/A	More Deta
CVE-2026-107266	Missing Authorization vulnerability in Drupal Views Share allows Forceful Browsing. This issue affects Views Share versions: from 0.0.0 to 2.0.1.	N/A	More Deta
CVE-2026-114531	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Swiper formatter allows Stored XSS. This issue affects Swiper formatter versions: from 0.0.0 to 2.1.2, from 3.0.1 to 3.1.0.	N/A	More Deta
CVE-2026-108097	Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection') vulnerability in Drupal Drupal core allows Reflection Injection. This issue affects Drupal core versions: from 8.9.0 to 10.6.19, from 11.0.0 to 11.3.19, from 11.4.0 to 11.4.10, from 12.0.0-alpha1 to 12.0.0-beta2.	N/A	More Deta
CVE-2026-108099	Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection') vulnerability in Drupal Entity List allows Reflection Injection. This issue affects Entity List versions: from 0.0.0 to 3.0.10.	N/A	More Deta
CVE-2026-108514	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Drupal core allows Cross-Site Scripting (XSS). This issue affects Drupal core versions: from 10.3.0 to 10.6.19, from 11.0.0 to 11.3.19, from 11.4.0 to 11.4.10, from 12.0.0-alpha1 to 12.0.0-beta2.	N/A	More Deta
CVE-2026-108515	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Drupal core allows Cross-Site Scripting (XSS). This issue affects Drupal core versions: from 8.9.0 to 10.6.19, from 11.0.0 to 11.3.19, from 11.4.0 to 11.4.10, from 12.0.0-alpha1 to 12.0.0-beta2.	N/A	More Deta
CVE-2026-110738	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Gin Admin Theme allows Cross-Site Scripting (XSS). This issue affects Gin Admin Theme versions: from 0.0.0 to 4.1.4, from 5.0.0 to 5.0.16.	N/A	More Deta
CVE-2026-114523	Improper Neutralization of Special Elements used in an OS Command ("OS Command Injection") vulnerability in Drupal Ffmpeg Image Toolkit allows OS Command Injection. This issue affects Ffmpeg Image Toolkit versions: from 0.0.0 to 1.0.3.	N/A	More Deta
CVE-2026-114524	Privilege Defined With Unsafe Actions vulnerability in Drupal Custom Formatters allows Privilege Escalation. This issue affects Custom Formatters versions: from 0.0.0 to 4.2.1.	N/A	More Deta
CVE-2026-114525	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal ABC allows Stored XSS. This issue affects ABC versions: from 0.0.0 to 1.25.0, from 2.0.0 to 2.0.1.	N/A	More Deta
CVE-2026-114526	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Black Hole allows Stored XSS. This issue affects Black Hole versions: from 0.0.0 to 1.26.0, from 2.0.0 to 2.0.1.	N/A	More Deta
CVE-2026-114527	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal UI Icons allows Cross-Site Scripting (XSS). This issue affects UI Icons versions: from 0.0.0 to 1.1.3, from 2.0.0 to 2.0.2.	N/A	More Deta

CVE-2026-114528	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Zero Point allows Stored XSS. This issue affects Zero Point versions: from 0.0.0 to 1.30.0, from 2.0.0 to 2.0.1.	N/A	More Deta
CVE-2026-114529	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal CSV Field allows Stored XSS. This issue affects CSV Field versions: from 0.0.0 to 2.0.10, from 3.0.0 to 3.0.7.	N/A	More Deta
CVE-2026-114530	Incorrect Authorization vulnerability in Drupal Dopup allows Forceful Browsing. This issue affects Dopup versions: from 0.0.0 to 1.0.7.	N/A	More Deta
CVE-2026-117717	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117719	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117789	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117720	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117772	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117771	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2025-62839	An use of hard-coded cryptographic key vulnerability has been reported to affect HBS 3 Hybrid Backup Sync and Hybrid Backup Sync. If exploited, the vulnerability could allow remote attackers to compromise the security of the system. We have already fixed the vulnerability in the following version: HBS 3 Hybrid Backup Sync 26.4.0.521 and later Hybrid Backup Sync 26.4.0.521 and later Hybrid Backup Sync 26.4.1.563 and later	N/A	More Deta
CVE-2025-62841	An use of hard-coded cryptographic key vulnerability has been reported to affect HBS 3 Hybrid Backup Sync and Hybrid Backup Sync. If exploited, the vulnerability could allow remote attackers to compromise the security of the system. We have already fixed the vulnerability in the following version: HBS 3 Hybrid Backup Sync 26.4.0.521 and later Hybrid Backup Sync 26.4.0.521 and later Hybrid Backup Sync 26.4.1.563 and later	N/A	More Deta
CVE-2026-117174	Rejected reason: VUL-2026-008368 為先回報之相同問題	N/A	More Deta
CVE-2026-114358	This vulnerability exists in the Radius Xenia M2M Platform due to insufficient validation of user supplied input in the password recovery functionality in the web management interface. An unauthenticated remote attacker could exploit this vulnerability by supplying crafted SQL query through input fields to the targeted system. Successful exploitation of this vulnerability could allow the attacker to gain unauthorized access to sensitive information, enumerate database structure or modify database records on the targeted system.	N/A	More Deta
CVE-2026-7190	A cross-site scripting (XSS) vulnerability in the ICTBroadcast software, which affects the demo environment. The vulnerability is found in the ‘login.php’ endpoint, where the ‘editForm[extension_username]’ parameter is reflected in the response without proper filtering. Successful exploitation of this vulnerability could allow an attacker to execute arbitrary JavaScript code in the victim’s browser once the victim accesses the malicious URL.	N/A	More Deta
CVE-2026-117770	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117769	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117768	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117611	Improper certificate validation in Checkmk <2.5.0p18, <2.4.0p39, <2.3.0p52 and 2.2.0 (EOL): the Certificate Authority stores bundled with "certifi" and "webpki-roots" include a root CA that trusts eMudhra (emSign) intermediate certificates whose private keys are public.	N/A	More Deta
CVE-2026-105031	When using the OpenSSL TLS implementation, both the pn_ssl_domain_set_trusted_ca_db() & pn_tls_config_set_trusted_certs() APIs added to rather than replaced the default system trust anchors. Leading to potentially trusting unexpected peer certificates. This can be worked around by setting the SSL_CERT_FILE environment variable for the application to /dev/null. This issue does not affect the Win32 SChannel TLS implementation. This issue affects Apache Qpid Proton C: through 0.40.0. Users are recommended to upgrade to version 0.41.1, which fixes the issue.	N/A	More Deta
CVE-2026-105042	A message body that is deeply nested and decoded by pn_message_body() could overflow the stack and cause a crash. This issue affects Apache Qpid Proton C: through 0.40.0. Users are recommended to upgrade to version 0.41.1, which fixes the issue.	N/A	More Deta
CVE-2026-117767	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta

CVE-2026-114230	When dispatching SASL frames to authenticate the peer, Proton will also dispatch AMQP frames if they claim to be SASL frames. This allows authentication bypass. However there will be no user name set so the effects depend on how the application deals with this condition - which otherwise means that authentication has not completed yet. This issue affects Apache Qpid Proton C: through 0.40.0. Users are recommended to upgrade to version 0.41.1, which fixes the issue.	N/A	More Deta
CVE-2026-117766	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-115942	A misconfigured wildcard TLS certificate causes a stack read overflow. This issue does not affect any wildcard certificate issued to the RFC9525 standard - the fix only accepts certificates that comply to this standard. This issue affects Apache Qpid Proton C: through 0.40.0. Users are recommended to upgrade to version 0.41.1, which fixes the issue.	N/A	More Deta
CVE-2026-117765	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117764	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-103665	The installer for Yamaha LAN Monitor for Windows provided by Yamaha Corporation may insecurely load Dynamic Link Libraries (DLLs). When the installer is launched in a directory containing a specially crafted DLL file, the malicious DLL may be loaded, resulting in arbitrary code execution with administrative privileges.	N/A	More Deta
CVE-2026-117763	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117762	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117761	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117760	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-5697	Stored Cross-Site Scripting (XSS) vulnerability in SABBATIC application that allows an attacker to store JavaScript code so that when a user views the page, code can be executed in the victim's browser. The list of assigned parameters and identifiers is as follows: parameter 'nombre' in '/usuario' endpoint;	N/A	More Deta
CVE-2026-5698	Stored Cross-Site Scripting (XSS) vulnerability in SABBATIC application that allows an attacker to store JavaScript code so that when a user views the page, code can be executed in the victim's browser. The list of assigned parameters and identifiers is as follows: parameters 'titulo_es' and 'add_etiquetas%5B%5D' in '/categorías' endpoint;	N/A	More Deta
CVE-2026-5699	Stored Cross-Site Scripting (XSS) vulnerability in SABBATIC application that allows an attacker to store JavaScript code so that when a user views the page, code can be executed in the victim's browser. The list of assigned parameters and identifiers is as follows: parameter 'companyName' in /empresa endpoint;	N/A	More Deta
CVE-2026-5700	Stored Cross-Site Scripting (XSS) vulnerability in SABBATIC application that allows an attacker to store JavaScript code so that when a user views the page, code can be executed in the victim's browser. The list of assigned parameters and identifiers is as follows: parameter 'observaciones' in /mis-gastos endpoint.	N/A	More Deta
CVE-2026-5702	Cross-Site Request Forgery (CSRF) vulnerability in SABBATIC application that allows an attacker can trick an authenticated user into clicking a malicious link or loading a page that sends unauthorized requests to a vulnerable endpoint.	N/A	More Deta
CVE-2026-117773	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117774	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117775	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-111575	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Deta
CVE-2026-117788	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117787	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117786	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta

CVE-2026-117785	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117784	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117783	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-57448	Blombooru is a self-hosted personal booru for organizing and tagging private image collections. Prior to 1.40.0, the administrator-only `GET /proxy-image` endpoint, exposed as `/api/booru-import/proxy-image`, accepts a `url` query parameter and fetches it server-side without meaningful destination validation. `proxy_image()` in `backend/app/routes/booru_import.py` only checks whether the value starts with http, then uses `get_client_for_url` or `requests.get` and streams the response. Private, loopback and link-local addresses are not blocked, and automatically followed redirects can move a request from a trusted domain to an internal address. An authenticated administrator can enumerate internal services and access cloud instance metadata, potentially disclosing IAM credentials and crossing the application's intended cloud or network trust boundary. The reporter also observed a hanging recursive self-request. Administrator authentication remains a prerequisite; this is not an anonymous proxy. This issue is fixed in version 1.40.0.	N/A	More Deta
CVE-2026-61546	AnkiMCP is an Anki addon that implements an MCP server, enabling AI assistants to interact with the Anki flashcard application. Prior to version 0.21.0, `anki_mcp_server/mcp_server.py` globally disables FastMCP DNS-rebinding protection through `TransportSecuritySettings` with `enable_dns_rebinding_protection=False`, including for the default local Streamable HTTP listener. The defaults in `anki_mcp_server/config.py` enable `http_enabled` on `127.0.0.1:3141`, with an empty `http_path` selecting the root endpoint. No bearer token, API key, session secret, strict `Host` allowlist or strict `Origin` allowlist is enforced before `initialize`, `tools/list` and `tools/call` reach MCP dispatch. A victim who visits a malicious web page while Anki and the listener are running can have browser requests rebound to loopback, allowing the attacker to `initialize` MCP, enumerate tools, read the local collection, and perform enabled non-destructive note/deck creation or updates. The attacker needs neither LAN position nor a local process. Available operations depend on enabled tool filters; destructive tools are hidden unless `enabled_destructive_tools` is opted into, limiting deletion-level impact but not the exposed read/write operations. The reported harness confirms real MCP tool dispatch with substituted Anki bridge responses rather than demonstrating destructive changes to a real collection. Disabling protection for tunnels/proxies also disables it for the normal loopback configuration. This issue is fixed in version 0.21.0.	N/A	More Deta
CVE-2026-117782	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117781	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117780	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-111478	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Deta
CVE-2026-111486	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Deta
CVE-2026-55561	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments. Prior to 1.7.2-beta-1, guest users can approve or reject quotes belonging to any client, not just their assigned clients. The `approve()` and `reject()` methods in the Guest Quotes controller, `application/modules/guest/controllers/Quotes.php`, call `approve_quote_by_id($quote_id)` and `reject_quote_by_id($quote_id)` directly without the `where_in('ip_quotes.client_id', $this->user_clients)` scoping that sibling methods use. A guest user assigned to one client can change another client's quote status by supplying sequential integer `quote_id` values, and `email_quote_status()` also sends notification emails. Additionally, `generate_pdf()` calls `mark_viewed($quote_id)` before checking the client scope, allowing a guest user to mark another client's quote as viewed. These issues are fixed in version 1.7.2-beta-1 and the subsequent stable version 1.7.2.	N/A	More Deta
CVE-2026-117776	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117779	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-86983	A remote attacker may be able to terminate a process that passes attacker-controlled input to the P-384 VOPRF API without bounding its length. This vulnerability is addressed in swift-crypto version 5.0.3.	N/A	More Deta
CVE-2026-113957	An attacker who controls the registry, a mirror, or the network path to it may be able to serve arbitrary image content in response to a pull by digest, so that a user runs an image other than the one they pinned. The fix compares the returned digest to the pinned digest and fails the pull on a mismatch. Tag pulls are exempt, because a tag is mutable by design. The fix also verifies the hash of manifests and blobs when they are fetched. This vulnerability is addressed in container version 1.6.0 and containerization version 0.52.1.	N/A	More Deta
CVE-2026-21157	Improper input validation in Bixby prior to version 4.0.85.6 allows privileged local attackers to launch arbitrary activity.	N/A	More Deta
CVE-2026-117778	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-	In openEQUELLA before 2026.1, the pre-login notice image upload endpoint (PUT /api/preloginnotice/image/{name}) does not validate the type of		

2026-16889	uploaded files and serves them with a Content-Type derived from the supplied filename. A user holding the EDIT_SYSTEM_SETTINGS permission can upload an HTML file that is then served as text/html from the openEQUELLA origin, resulting in stored cross-site scripting. Unauthenticated exploitation is possible where EDIT_SYSTEM_SETTINGS has been granted to the guest user or everyone.	N/A	More Deta
CVE-2026-66088	In openEQUELLA before 2026.1, the system.execute() function available to the scripting engine runs supplied operating system commands without validation or an allow-list of permitted executables. A user able to create or edit scripts can use it to execute arbitrary commands with the privileges of the openEQUELLA service account.	N/A	More Deta
CVE-2026-66089	In openEQUELLA before 2026.1, the SOAP API parses XML supplied in the stopEdit operation with a parser that resolves external entities. This allows an attacker to read arbitrary files accessible to the openEQUELLA service or cause the server to issue requests to attacker-specified locations (SSRF).	N/A	More Deta
CVE-2026-66090	In openEQUELLA before 2026.1, the XML parser used for item metadata does not disable external entity resolution. A user permitted to create items (CREATE_ITEM) can submit crafted XML to POST /api/item and cause the server to read arbitrary files accessible to the openEQUELLA service, or make requests to attacker-specified locations (SSRF), including cloud instance metadata services.	N/A	More Deta
CVE-2026-66091	In openEQUELLA before 2026.1, the GET /api/userquery/userinfobackup endpoint performs no authentication or authorisation check. An unauthenticated attacker who supplies another user's uniqueId can retrieve that user's stored personal details (username, first name, last name and email address) within the same institution.	N/A	More Deta
CVE-2026-66092	In openEQUELLA before 2026.2, the pre-login notice is stored as HTML and rendered on the legacy logon page without encoding or sanitisation. A user holding the EDIT_SYSTEM_SETTINGS permission can set a notice containing an arbitrary script (PUT /api/preloginnotice), resulting in stored cross-site scripting on the login page. Unauthenticated exploitation is possible where EDIT_SYSTEM_SETTINGS has been granted to the guest user or Everyone	N/A	More Deta
CVE-2026-118426	In affected versions of Octopus Server with the LDAP authentication provider enabled, any authenticated user could call the LDAP user search and LDAP group search.	N/A	More Deta
CVE-2026-117777	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-97860	YMS-VPN8 and YMS-VPN8-CP provided by Yamaha Corporation register Windows services with unquoted file paths. A user who has write permissions on the system drive may be able to execute arbitrary code with SYSTEM privileges.	N/A	More Deta
CVE-2026-113688	Server-side request forgery in the SmartIT URL-based attachment feature of BMC IT Service Management Suite versions 25.3.01, 25.4.01, and 26.1.01 allows authenticated users to make server-side requests to internal services and observe response information.	N/A	More Deta
CVE-2026-113689	Stored cross-site scripting in the SmartIT work-notes feature of BMC IT Service Management Suite versions 25.3.01, 25.4.01, and 26.1.01 allows authenticated users to execute stored scripts in other users' browsers.	N/A	More Deta
CVE-2026-111735	P-Net before 1.0.3 contains an integer underflow in pf_cpm_c_data_ind(). When handling a received cyclic data frame while the consumer is in the FRUN or RUN state, the offset of the APDU status was computed as the frame length minus 4 using 16-bit arithmetic, without checking that the frame is long enough. A crafted short frame makes the offset wrap around, so the function reads outside the receive buffer. This can cause a crash (denial of service) or disclose memory content.	N/A	More Deta
CVE-2026-117735	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117734	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117733	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117732	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117731	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117730	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117729	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117728	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-111730	P-Net before 1.0.3 does not validate the LengthPeerStationName field of a CheckPeers block in get_check_peer(). The received length (up to 255) was used to copy data into the 241-byte peer station name buffer and to place the terminating NUL byte, so a crafted block writes up to 15 bytes past the end of the buffer. This can lead to a crash (denial of service) or potentially arbitrary code execution. Requires establishment of session that needs ADJACENT network access.	N/A	More Deta
CVE-2026-	P-Net before 1.0.3 enters an infinite loop when handling a read request for the PDPortDataCheck record with subslot 0 (whole module). The loop over the ports never advanced to the next port, so the request never completes and the device stops responding. A remote unauthenticated	N/A	More

111731	attacker can use this to cause a denial of service.		Deta
CVE-2026-111732	P-Net before 1.0.3, when built with PNET_OPTION_AR_VENDOR_BLOCKS enabled, parses a data length from a field of the ARVendorBlock request that is not part of the block definition and uses it as the number of bytes to copy into a fixed-size buffer, without comparing it with the buffer size or the block length. A crafted Connect request causes an out-of-bounds write. This can lead to a crash (denial of service) or potentially arbitrary code execution. This option is disabled by default.	N/A	More Deta
CVE-2026-111733	P-Net before 1.0.3 dereferences a NULL AR pointer when handling an implicit read request without a valid target AR UUID for a record index that requires an AR (AR specific indices 0xE000-0xEFFF, and the expected identification data of a slot or subslot). A remote unauthenticated attacker can send such a request to crash the device (denial of service).	N/A	More Deta
CVE-2026-111734	P-Net before 1.0.3 does not validate the length of a received Ethernet frame in pf_eth_recv() before reading the EtherType, any VLAN tags and the PROFINET FrameID. The VLAN tag loop had no upper bound, so a truncated frame, or a frame consisting only of VLAN tags, makes the function read past the end of the receive buffer. This can cause a crash (denial of service) or disclose memory content.	N/A	More Deta
CVE-2026-111736	P-Net before 1.0.3 dereferences a NULL AR pointer in pf_fspm_cm_read_ind() when handling an implicit read request without a valid target AR UUID for a user specific record index, if the application has registered a read callback. A remote unauthenticated attacker can send such a request to crash the device (denial of service).	N/A	More Deta
CVE-2026-117737	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-112200	P-Net before 1.0.3 does not release the Application Relationship (AR) and the RPC session when an RPC request is rejected because its data representation has incorrect endianness. The session and its AR remain allocated, so repeated requests exhaust the available sessions. Once they are exhausted the device no longer answers new RPC requests, including Connect, until it is restarted. A remote unauthenticated attacker can use this to cause a denial of service.	N/A	More Deta
CVE-2026-112255	Initialization of a resource with an insecure default vulnerability in OpenText Advanced Authentication Server allows Excessive Allocation. This issue affects Advanced Authentication Server: from 6.4.0.0 through 6.4.3.x, from 6.5.0.0 through 6.5.0.x, and from 6.6.0.0 through 6.6.1.0. The fix for this is issue is to create a secure configuration. The 6.6.2.0 release has a best practice entry if the configuration is unsecure. A secure configuration is to NOT allow creation/recreation of Unauthenticated Endpoints. If creation/recreation of Unauthenticated Endpoints is required, you should only allow it from trusted networks. To remedy this issue, change your configuration to NOT allow creation/recreation of Unauthenticated Endpoints. If you require Unauthenticated Endpoints, you MUST change your configuration to use a non-empty whitelist to specify the trusted networks. An empty whitelist will allow all networks to create/recreate endpoints.	N/A	More Deta
CVE-2026-112256	Acceptance of extraneous untrusted data with trusted data vulnerability in OpenText Advanced Authentication Server allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Advanced Authentication Server: from 6.4.0.0 through 6.4.3.8, from 6.5.0.0 through 6.5.0.10, and from 6.6.0.0 through 6.6.1.0.	N/A	More Deta
CVE-2026-117727	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-115793	P-Net before 1.0.3 does not release the RPC session allocated for an RPC request that names an unknown interface or object UUID, and does not start a timeout for it. Repeated requests with different activity UUIDs exhaust the available sessions. Once they are exhausted the device no longer answers new RPC requests, including Endpoint Mapper Lookup and Connect, until it is restarted. A remote unauthenticated attacker can use this to cause a denial of service.	N/A	More Deta
CVE-2026-115794	P-Net before 1.0.3 passes the application alarm callback a data length derived from the variable part length field of a received RTA alarm frame without checking it against the length of the received frame. A short frame can make the callback receive a length of up to 65507 bytes. An application that copies the reported number of bytes reads past the end of the receive buffer. The attacker must have established an Application Relationship and requires ADJACENT network access. Applications that do not use the alarm data are not affected.	N/A	More Deta
CVE-2026-115795	P-Net before 1.0.3 does not check that a complete block header is present in the received data before reading the next block in DCP Set and Identify requests. If the last block ends at the end of the receive buffer, the block length of the following block is read past the end of the buffer. In addition, a DCP Set block with a length smaller than the two-byte block qualifier makes the length underflow, so the block is processed with a length of 65534 bytes. This can cause a crash (denial of service) or disclose a small amount of memory content. Requires ADJACENT network access.	N/A	More Deta
CVE-2026-117726	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117725	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117724	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117723	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117722	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117721	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117736	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta

CVE-2026-117738	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-113690	Stored cross-site scripting in the SmartIT attachment feature of BMC IT Service Management Suite versions 25.3.01, 25.4.01, and 26.1.01 allows authenticated users to execute uploaded script content in other users' browsers.	N/A	More Deta
CVE-2026-117753	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117759	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117758	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-113691	Stored cross-site scripting in the SmartIT knowledge-article feature of BMC IT Service Management Suite versions 25.3.01, 25.4.01, and 26.1.01 allows authenticated users to execute stored scripts in other users' browsers.	N/A	More Deta
CVE-2026-113692	Path traversal in the SmartIT file-management feature of BMC IT Service Management Suite versions 25.3.01, 25.4.01, and 26.1.01 allows authenticated administrators to read files outside the intended directory.	N/A	More Deta
CVE-2026-113693	Exposure of sensitive information in the SmartIT system-account settings of BMC IT Service Management Suite versions 25.3.01, 25.4.01, and 26.1.01 allows authenticated users to retrieve a system username and encrypted password value.	N/A	More Deta
CVE-2026-113694	Improper authorization in the SmartIT user attachment feature of BMC IT Service Management Suite versions 25.3.01, 25.4.01, and 26.1.01 allows authenticated users to access or modify attachment resources belonging to other users.	N/A	More Deta
CVE-2026-113695	Reflected cross-site scripting in the SmartIT inline-image attachment feature of BMC IT Service Management Suite versions 25.3.01, 25.4.01, and 26.1.01 allows authenticated users to inject script content into HTML responses viewed by another user.	N/A	More Deta
CVE-2026-113696	Improper authorization in the SmartIT change approval feature of BMC IT Service Management Suite versions 25.3.01, 25.4.01, and 26.1.01 allows authenticated users to make unauthorized changes to approval state and bypass intended approval restrictions.	N/A	More Deta
CVE-2026-113697	Reflected cross-site scripting in the agent query feature of BMC Helix Operations Management 25.4.00 allows authenticated attackers to execute script in another user's browser after that user opens a crafted link.	N/A	More Deta
CVE-2026-117757	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117756	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117755	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117754	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117752	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117739	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117751	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117750	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117749	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117748	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-			

2026-117747	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117746	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117745	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117744	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117743	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117742	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-117741	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-106036	Szafir accepts any client or server certificate without performing certificate and hostname validation, allowing HTTPS connections without authenticating the remote server. An attacker can provide an arbitrary SSL/TLS certificate and cause the application to download an update file from their server. This issue was fixed in version 2.0 build 708.	N/A	More Deta
CVE-2026-117740	Rejected reason: Reserved in error; never associated with a vulnerability.	N/A	More Deta
CVE-2026-111477	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Deta