SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 02 September 2026

Generated on 02 September 2026

SingCERT's Security Bulletin summarises the list of vulnerabilities collated from the National Institute of Standards and Technology (NIST)'s National Vulnerability Database (NVD) in the past week.

The vulnerabilities are tabled based on severity, in accordance to their CVSSv3 base scores:

Critical	vulnerabilities with a base score of 9.0 to 10.0
High	vulnerabilities with a base score of 7.0 to 8.9
Medium	vulnerabilities with a base score of 4.0 to 6.9
Low	vulnerabilities with a base score of 0.1 to 3.9
None	vulnerabilities with a base score of 0.0

For those vulnerabilities without assigned CVSS scores, please visit NVD for the updated CVSS vulnerability entries.

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2026-81735	startServer.ts in the mcp-http-server package of UI-TARS-desktop defaulted its listen address to '::' when no host was given, so startSseAndStreamableHttpMcpServer bound the Streamable HTTP and SSE MCP transports to every interface, and its authentication middleware was optional: middlewares are applied only when a caller supplies them. The @agent-infra/mcp-server-commands and @agent-infra/mcp-server-filesystem entry points call startSseAndStreamableHttpMcpServer with a host and port alone and pass no middleware, so neither server required a credential. The commands server exposes a run_command tool that hands its caller-supplied command string to promisify(child_process.exec), so any unauthenticated client able to reach the port could run arbitrary commands as the user running the server, and the filesystem server exposed its file read and write tools on the same terms. The listen default became 127.0.0.1 in commit c2ad42e3eb9b27830db41a3e6f51ca7179d9b168; the package version stayed at 1.2.4 across that change, so the boundary is the commit rather than a release.	10.0	More Details
CVE-2026-81096	ToolUniverse ran caller-supplied Python inside a sandbox that could be escaped, on a server that required no authentication. The executor behind the python_code_executor tool, in python_executor_tool.py, inspected the submitted source for a denied list of attribute names and calls but left the attribute-lookup builtins available and did not stop a dunder attribute reached through a string lookup or through a module already permitted, so a caller could walk from a literal's class to its base and enumerate subclasses to obtain a reference to the process and subprocess modules. A per-call argument also let the caller widen the import allow-list before the inspection ran. The HTTP and MCP servers in http_api_server.py and smcp_server.py bound to every interface with debugging enabled and no authentication, so any caller able to reach the port executed code as the server process. Version 1.3.0 adds bearer-token authentication, defaults the bind address to loopback, and hardens the attribute checks.	10.0	More Details
CVE-2026-54745	Kubeflow Pipelines enables users to build and deploy portable, scalable machine learning workflows. Prior to 2.17.0, the Kubeflow Pipelines frontend exposes an unauthenticated server-side request forgery vulnerability through the /_proxy/ route in frontend/server/proxy-middleware.ts. The _routePathWithReferer() function accepts an arbitrary attacker-controlled HTTP or HTTPS target and passes its origin to createProxyMiddleware without a host allowlist or filtering for loopback, link-local, RFC1918, or cluster-local addresses. The route remains outside the authorization middleware when ENABLE_AUTHZ=true and is reachable through /apis/v1beta1/_proxy/, /apis/v2beta1/_proxy/, /pipeline/apis/v1beta1/_proxy/, and /pipeline/apis/v2beta1/_proxy/, including through a crafted Referer header. Requests can forward attacker-controlled methods, headers such as Authorization, Cookie, and X-Forwarded-For, and POST bodies to reachable internal services, while returning the upstream response to the unauthenticated client. This can expose cloud metadata credentials, Kubernetes or service APIs, and other cluster-internal endpoints to unauthorized read or modification. This issue is fixed in version 2.17.0.	10.0	More Details
CVE-2026-	Deserialization of Untrusted Data vulnerability in Liquid Web / StellarWP GiveWP allows Object Injection. This issue affects GiveWP: from n/a through 4.16.7.1.	10.0	More Details

82222			
CVE-2026-82456	argocd-mcp 0.8.0 binds its HTTP transport to every network interface and accepts MCP sessions without requiring caller credentials when ARGOCD_API_TOKEN is configured. Attackers who can reach the listener can invoke the full tool surface using the operator's stored token to create applications, request syncs, and modify Argo CD resources.	10.0	More Details
CVE-2026-82542	A weakness has been identified in Tenda HG10 300001138. Affected by this issue is the function formIPv6Routing of the file /boaform/admin/formIPv6Routing of the component Boa Web Server. This manipulation of the argument destNet causes buffer overflow. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks.	10.0	More Details
CVE-2026-82693	A vulnerability was determined in Tenda AC1206 15.03.06.23. This vulnerability affects the function TendaTelnet of the file /goform/telnet of the component Web UI. Executing a manipulation can lead to missing authentication. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized.	10.0	More Details
CVE-2026-82695	A security flaw has been discovered in Tenda AC18 15.03.05.19. Impacted is an unknown function of the file /goform/telnet of the component Telnet Handler. The manipulation results in missing authentication. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks.	10.0	More Details
CVE-2026-77554	A malicious actor with access to the network could exploit an Improper Input Validation vulnerability found in UniFi Talk Application to execute a Command Injection on the host device.	10.0	More Details
CVE-2026-82970	Unrestricted Upload of File with Dangerous Type vulnerability in WP Legal Pages WP Cookie Notice for GDPR, CCPA & ePrivacy Consent allows Using Malicious Files. This issue affects WP Cookie Notice for GDPR, CCPA & ePrivacy Consent: from n/a through 4.4.1.	10.0	More Details
CVE-2026-77550	A malicious actor with access to the network could exploit an Improper Neutralization of CRLF Sequences vulnerability found in certain devices running UniFi OS to bypass authentication to such UniFi OS devices or instances.	10.0	More Details
CVE-2026-82694	A vulnerability was identified in Tenda AC1206 15.03.06.23. This issue affects the function R7WebsSecurityHandler of the file /goform/ate of the component Web UI. The manipulation leads to missing authentication. The attack can be initiated remotely. The exploit is publicly available and might be used.	10.0	More Details
CVE-2026-77537	A malicious actor with access to the network could exploit an Improper Input Validation vulnerability found in UniFi Protect Application to execute a Command Injection on the host device.	10.0	More Details
CVE-2026-55634	Pimcore is an Open Source Data & Experience Management Platform. Prior to 11.5.19, 12.3.10, and 2026.1.6, the class-definition import endpoint /pimcore-studio/api/class/definition/configuration-view/detail/{id}/import accepts a DataObject field name that is emitted without an identifier allowlist by lib/DataObject/ClassBuilder/FieldDefinitionPropertiesBuilder.php into generated PHP properties and by models/DataObject/ClassDefinition/Helper/Dao.php into ALTER TABLE identifiers. An authenticated user with the objects permission can inject PHP syntax into the generated DataObject class, causing attacker-controlled code in generated var/classes/DataObject/.php files to run when an object of that class is instantiated, and can also inject SQL identifier content into schema-changing statements. The central models/DataObject/ClassDefinition/Data.php::setName() validation did not reject semicolons, braces, backticks, spaces, or other non-identifier characters. This issue is fixed in versions 11.5.19, 12.3.10, and 2026.1.6.	9.9	More Details
CVE-2026-82592	A vulnerability was detected in D-Link DIR-825M 1.1.8. This affects the function sub_46725C of the file /boafrm/formDiskFormat of the component Disk Formatting Handler Endpoint. The manipulation of the argument partition results in stack-based buffer overflow. The attack can be executed remotely. The exploit is now public and may be used.	9.9	More Details
CVE-2026-82874	ToolJet before v3.16.208 fails to validate that authenticated users belong to the organization specified in the organizationId path parameter of tooljet-db endpoints, allowing any Builder user to read, modify, and delete tables across tenant boundaries. Attackers can extract victim organization IDs from public app endpoints, then exploit schema operation endpoints to disclose table schemas, plant malicious tables, corrupt existing schemas, or permanently destroy victim data without any relationship to the target organization.	9.9	More Details
CVE-2026-82689	A vulnerability was detected in D-Link DNS-320L, DNS-327L, DNS-340L and DNS-345 up to 20260717. Affected is an unknown function of the file /cgi-bin/isomount_mgr.cgi of the component ISO Image Handler. The manipulation of the argument upIsoRootPath results in os command injection. The attack can be executed remotely. The exploit is now public and may be used.	9.9	More Details
CVE-2026-82692	A vulnerability was found in D-Link DNS-340L and DNS-345 up to 20260717. This affects an unknown part of the file /cgi-bin/iscsi_mgr.cgi. Performing a manipulation of the argument alias/username/password/volume_location results in os command injection. It is possible to initiate the attack remotely. The exploit has been made public and could be used.	9.9	More Details
CVE-2026-77534	A malicious actor with access to the network and low privileges could exploit an Improper Access Control vulnerability found in certain devices running UniFi OS to escalate privileges within such UniFi OS devices or instances.	9.9	More Details

CVE-2026-55565	Yamcs is a mission control framework. Prior to 5.12.8 and 5.13.2, Yamcs LikeExpression.fillCode_getValueReturn in yamcs-core/src/main/java/org/yamcs/yarch/streamsql/LikeExpression.java inserts an unescaped LIKE pattern into Java source compiled by Expression.getCompiledExpression through SimpleCompiler.cook instead of applying ValueExpression.escapeJavaString. The pattern can originate from POST /api/archive/{instance}:executeSql, POST /api/archive/{instance}:streamSql, POST /api/archive/{instance}/tables/{table}:readRows, GET /api/archive/{instance}/events, or activity searches, including paths available with ReadTables, ReadEvents, or ReadActivities. A quote in the pattern can inject Java that runs as the Yamcs server process. This issue is fixed in versions 5.12.8 and 5.13.2.	9.9	More Details
CVE-2026-82616	A vulnerability was found in TOTOLINK NR1800X 9.1.0u.6681_B20230703. Impacted is the function setUploadSetting of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument FileName results in stack-based buffer overflow. The attack can be executed remotely. The exploit has been made public and could be used.	9.9	More Details
CVE-2026-77536	A malicious actor with access to the network and low privileges could exploit an Improper Access Control vulnerability found in certain devices running UniFi OS to escalate privileges within such UniFi OS devices or instances.	9.9	More Details
CVE-2026-77553	A malicious actor with access to the network and low privileges could exploit an Improper Access Control vulnerability found in UniFi Access Application to escalate privileges on the host device.	9.9	More Details
CVE-2026-19295	IBM Langflow OSS 1.0.0 through 1.11.1 allows an authenticated attacker to execute arbitrary operating system commands in the server process by saving a flow with a crafted type field value and triggering a build of a wrapper flow that references it. This allowed privilege escalation from "authenticated flow user" to arbitrary OS-level command execution under the server process identity, bypassing the LANGFLOW_ALLOW_CUSTOM_COMPONENTS=false policy control.	9.9	More Details
CVE-2026-82593	A flaw has been found in D-Link DIR-825M 1.1.8. This impacts the function sub_41802C of the file /boafrm/formLtefotaUpgradeFibocom of the component LTE Module Firmware Upgrade. This manipulation of the argument fota_url causes stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit has been published and may be used.	9.9	More Details
CVE-2026-79748	MCPHub is a unified hub for centrally managing and dynamically orchestrating multiple MCP servers/APIs into separate endpoints with flexible routing strategies. Prior to version 0.12.15, the POST /api/servers and PUT /api/servers/:name endpoints in MCPHub create/update MCP server configurations and then immediately spawn the configured stdio process via child_process.spawn. Authentication is required, but there is no authorization check restricting these endpoints to admins, and there is no allowlist/sanitization on the command and args fields. As a result, any authenticated non-admin user can submit a server configuration with command:"/bin/sh" (or any other binary) and arbitrary args, causing MCPHub to execute the attacker-controlled process as the MCPHub server's OS user (commonly root in the published Docker image and in npx/systemd deployments). This issue has been patched in version 0.12.15.	9.9	More Details
CVE-2026-77546	A malicious actor with access to the network and low privileges could exploit an Improper Input Validation vulnerability found in UniFi Access Application to execute a Command Injection on the host device.	9.9	More Details
CVE-2026-77543	A malicious actor with access to the network and low privileges could exploit an Improper Input Validation vulnerability found in UniFi Access Application to execute a Command Injection on the host device.	9.9	More Details
CVE-2026-18527	IBM Administration Runtime Expert for i 1R1M0 IBM Application Runtime Expert (ARE) for i could allow a remote attacker to gain elevated privileges, caused by ARE GUI component processing. An unauthenticated attacker can exploit this vulnerability to execute actions under another user's authenticated profile gaining elevated privileges on the IBM i system.	9.9	More Details
CVE-2026-77533	A malicious actor with access to the network and low privileges could exploit an Improper Input Validation vulnerability found in UniFi Protect Application to execute a Command Injection on the host device.	9.9	More Details
CVE-2026-77547	A malicious actor with access to the network and low privileges could exploit an Improper Input Validation vulnerability found in UniFi Access Application to execute a Command Injection on the host device.	9.9	More Details
CVE-2026-77548	A malicious actor with access to the network and low privileges could exploit an Improper Input Validation vulnerability found in UniFi Protect Application to execute a Command Injection on the host device.	9.9	More Details
CVE-2026-80714	In the Linux kernel, the following vulnerability has been resolved: ipvs: do not propagate one-packet flag to synced conns Synced connections can be created before their destination exists. When the destination is later added, ip_vs_bind_dest() copies connection flags from the destination into cp->flags. IP_VS_CONN_F_ONE_PACKET connections are not synced. If a synced connection inherits IP_VS_CONN_F_ONE_PACKET while it is already hashed, expiry can treat it as a one-packet connection and skip unlinking the existing conn_tab node, leaving stale hash nodes pointing at a freed struct ip_vs_conn. Drop IP_VS_CONN_F_ONE_PACKET from destination flags when binding synced connections.	9.8	More Details

CVE-2026-80694	In the Linux kernel, the following vulnerability has been resolved: net: ethernet: mtk_eth_soc: pass eth to mtk_handle_irq_rx in poll_controller mtk_handle_irq_rx expects a struct mtk_eth * (matching the request_irq cookie), but mtk_poll_controller incorrectly passed the net_device *. Calling ndo_poll_controller with CONFIG_NET_POLL_CONTROLLER enabled would then crash.	9.8	More Details
CVE-2026-30612	An issue in Time4 Popcorn for Windows <= 6.2.1.18 and Time4Popcorn for MacOS <= 6.2.1.17 and Time4Popcorn for Android <= 3.5.0.173 allows a remote attacker to execute arbitrary code via the updater.exe for windows, PT.updd on MacOS components	9.8	More Details
CVE-2026-51645	Incorrect access control in the getPasswordCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain the administrative username via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.8	More Details
CVE-2026-81578	An improper access control vulnerability exists in the web management interface of PaperCut MF and PaperCut NG. Under specific conditions, unauthenticated remote requests targeting administrative functions can trigger backend actions prior to the completion of access validation checks. This allows an unauthenticated remote attacker to modify certain system configurations.	9.8	More Details
CVE-2026-55559	Yamcs is a mission control framework. Prior to 5.12.8 and 5.13.2, Yamcs inserts templateArgs from POST /api/instances and PATCH /api/instances/{instance} into YAML through VarStatement.append in yamcs-core/src/main/java/org/yamcs/templating/VarStatement.java without YAML-context escaping. The rendered configuration is parsed by YamcsServer.createInstance and loaded by YamcsServerInstance, allowing an attacker to inject a services entry for org.yamcs.ProcessRunner. Deployments without security.yaml expose the operation through the guest superuser, while secured deployments require SystemPrivilege.CreateInstances. Successful exploitation executes commands as the Yamcs service account. This issue is fixed in versions 5.12.8 and 5.13.2.	9.8	More Details
CVE-2026-80681	In the Linux kernel, the following vulnerability has been resolved: vxlan: re-fetch eth header after route_shortcircuit() Before route_shortcircuit(), the eth header pointer is cached from eth_hdr(skb). Inside route_shortcircuit(), pskb_may_pull() can be called, which may reallocate skb->head. In this case, returning to vxlan_xmit() leaves the cached eth pointer pointing to freed memory, leading to a use-after-free when dereferencing eth->h_dest. Fix this by updating eth = eth_hdr(skb) after calling route_shortcircuit().	9.8	More Details
CVE-2026-35868	A Command Injection vulnerability exists in the bs_SetLimitCli_info function within the libshare.so library of LB-link Router AC2100_AZ3 V1.0.4. This flaw occurs due to insufficient validation and sanitization of user-supplied input before it is passed to a system-level command execution context. An attacker can exploit this vulnerability by injecting specially crafted shell metacharacters or payloads into the vulnerable parameter, resulting in the execution of arbitrary operating system commands.	9.8	More Details
CVE-2026-80674	In the Linux kernel, the following vulnerability has been resolved: ntfs: validate resident attribute lists and harden the validator A base inode's $ATTRIBUTE_LIST is sanity-checked by load_attribute_list() only on the non-resident path; ntfs_read_locked_inode() copies a *resident* attribute list into ni->attr_list with a plain memcpy() and no validation at all. Every subsequent walk of ni->attr_list -- ntfs_external_attr_find(), ntfs_inode_attach_all_extents() and ntfs_attrlist_need() -- then trusts the entries are well-formed and reads attr_list_entry fixed-header fields (lowest_vcn at offset 8, mft_reference at offset 16, and the name) with bounds that assume validation already happened. A crafted resident attribute list therefore reaches those walks unvalidated and can drive out-of-bounds reads of the attribute-list buffer. load_attribute_list() itself reads ale->name_offset (offset 7), ale->mft_reference (offset 16) and the name length under only an "al < al_start + size" bound, so its own validation loop can over-read the fixed header of a truncated trailing entry by a few bytes. Factor the per-entry validation into ntfs_attr_list_entry_is_valid(), which requires each entry's fixed header (offsetof(struct attr_list_entry, name)) to be in range before any field is dereferenced, that ale->length is a multiple of 8 covering the fixed header plus the name, and that the entry is in use and carries a live MFT reference. ntfs_attr_list_is_valid() walks the buffer with it and checks the entries tile it exactly. Use the list validator in load_attribute_list() (replacing the open-coded loop, closing its own over-read) and on the resident path in ntfs_read_locked_inode() (which previously skipped validation entirely); patches 2/3 reuse the per-entry helper at the other two attribute-list walks.	9.8	More Details
CVE-2026-80673	In the Linux kernel, the following vulnerability has been resolved: ntfs: bound the look-ahead attribute-list entry in ntfs_external_attr_find() When resolving an attribute lookup with a non-zero @lowest_vcn, ntfs_external_attr_find() peeks at the next $ATTRIBUTE_LIST entry to decide whether to keep searching, but bounds that not-yet-validated entry only with "(u8 *)next_al_entry + 6 < al_end" (which proves just bytes 0..6 are in range) and "(u8 *)next_al_entry + length <= al_end" with an attacker-controlled, non-8-aligned length. It then reads next_al_entry->lowest_vcn (an __le64 at offset 8) and the name at next_al_entry->name_offset, both of which can lie past al_end -- the exact end of the kvmalloc'd attribute-list buffer (allocated at the on-disk attr_list_size, no rounding). A crafted on-disk $ATTRIBUTE_LIST whose last entry sits a few bytes before al_end therefore yields a slab out-of-bounds read when the inode is read. Validate the look-ahead entry with ntfs_attr_list_entry_is_valid() (added in patch 1/3) before dereferencing lowest_vcn and the name, so the same fixed-header, length and name bounds the main attribute-list walk uses now guard this read too.	9.8	More Details
	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_conntrack_expect: use conntrack GC to reap expectations This patch replaces the timer API by GC worker approach for expectations, as it already happened in many other subsystems. Use the existing conntrack GC worker to iterate over the local list of expectations in the master conntrack to reap expired expectations. Check IPS_HELPER_BIT to run GC for expectations, set it on for nft_ct expectation which nevers sets it. Hold the expectation spinlock while iterating over the master conntrack expectation list to synchronize with nf_ct_remove_expectations(). This also performs runtime packet path garbage collection through the expectation insertion and lookup functions while walking over		

CVE-2026-80668	one of the chains of the global expectation hashtables. Unconfirmed conntrack entries are skipped since ct->ext can be reallocated and dying are skipped since those will be gone soon. Set on IPS_HELPER_BIT if the helper ct extension is added, then the new GC worker does not need to bump the ct refcount to check if the ct->ext helper is available. This removes the extra bump on the refcount for expectation timers, this allows to remove several nf_ct_expect_put() calls after the unlink, after this update only refcount remains at 1 while on the expectation hashes. This patch implicitly addresses a race with the existing timer API allowing an expectation to access a stale exp->master pointer which has been already released when expectation removal loses races with an expiring timer, ie. timer_del() reporting false. Add a new NF_CT_EXPECT_DEAD flag to reap this expectation via GC. This is needed by nf_conntrack_unexpect_related() which is called in error paths to invalidate newly created expectations that has been added into the hashes. These expectactions cannot be inmediately released as GC or nf_ct_remove_expectations() could race to make it. On expectation insert, the runtime GC reaps stale expectations before checking the expectation limit set by policy. Set current timestamp in nf_ct_expect_alloc(), then add the expectation policy timeout (or custom timeout specified added on top of this) to specify the expectation lifetime.	9.8	More Details
CVE-2026-35869	A Command Injection vulnerability exists in the bs_SetLimitCli_info function within the libshare.so library of LB-link Router AC450M V4.0.0. This flaw occurs due to insufficient validation and sanitization of user-supplied input before it is passed to a system-level command execution context. An attacker can exploit this vulnerability by injecting specially crafted shell metacharacters or payloads into the vulnerable parameter, resulting in the execution of arbitrary operating system commands.	9.8	More Details
CVE-2026-37751	An OS command injection vulnerability in the killSessionSync function (lib/agent-runtime.ts) of 23blocks-OS ai-maestro v0.24.17 allows attackers to execute arbitrary commands via a crafted input.	9.8	More Details
CVE-2026-37004	BerriAI litellm <=1.82.4 is vulnerable to Server-Side Template Injection (SSTI), which allows unauthenticated remote attackers to execute arbitrary OS commands via a crafted dotprompt_content parameter in the /prompts/test endpoint due to use of an unsandboxed jinja2.Environment.	9.8	More Details
CVE-2026-80634	In the Linux kernel, the following vulnerability has been resolved: netfilter: flowtable: avoid num_encaps underflow on bridge VLAN untag The DEV_PATH_BR_VLAN_UNTAG case post-decrements info->num_encaps inside WARN_ON_ONCE(). num_encaps is u8, so if it's already 0 the decrement still happens and wraps it to 255. The break only leaves the inner switch -- a later path entry can set info->indev back to a real device, and we end up returning with num_encaps == 255. nft_dev_forward_path() then walks info.encap[] (size 2) up to num_encaps, which means an OOB stack read and a bogus count copied into the route descriptor. Should only happen on a malformed bridge path stack, hence the WARN, but worth handling sanely. Move the decrement out of the WARN. [While at this, remove the WARN_ON_ONCE since this can only happen with a buggy bridge path stack --pablo].	9.8	More Details
CVE-2026-76943	Xiiaozet LK100Wt contains an authentication weakness within an administrative service that may allow an attacker to bypass intended access controls and obtain command execution capabilities. Successful exploitation could allow unauthorized interaction with privileged functionality and may lead to complete device compromise.	9.8	More Details
CVE-2026-37007	A vulnerability in FileWriterTool in crewai-tools <= 1.10.2rc1 allows a remote attacker to achieve code execution via malicious path traversal sequences in the filename argument.	9.8	More Details
CVE-2026-59313	Spring MVC applications using the functional web framework are vulnerable to stream corruption when using Server-Sent Events (SSE). Spring Framework 7.0.0 - 7.0.8 Spring Framework 6.2.0 - 6.2.19 Spring Framework 6.1.0 - 6.1.28 Spring Framework 6.0.0 - 6.0.30 Spring Framework 5.3.0 - 5.3.49	9.8	More Details
CVE-2026-69658	MQTT credentials and control traffic are transmitted in cleartext, exposing sensitive information to network-level attackers. This may enable unauthorized device impersonation and disruption of messaging functions.	9.8	More Details
CVE-2026-71187	The Ebyte device relies on client side authentication logic that can be reproduced by unauthenticated users. An attacker may generate valid authentication requests and bypass authentication to obtain administrative access to the device.	9.8	More Details
CVE-2026-73125	Ebyte device web management interface does not consistently enforce authentication before granting access to administrative functionality. An unauthenticated remote attacker could access sensitive configuration information, modify device settings, or disrupt availability.	9.8	More Details
CVE-2026-75337	The static resource interface /api/static/{deployKey}/ of Yu AI Code Mother v4.3 is vulnerable to path traversal. The user-controlled path is concatenated to the preview root directory without any normalization, allowing anonymous attackers to read files outside the preview root.	9.8	More Details
CVE-2026-76179	An improper protection of authentication tokens vulnerability exists in certain Ebyte gateway products. Authentication tokens used by the web management interface are insufficiently protected during client-side session handling, which may allow an attacker with access to exposed session information to obtain and reuse a valid token. Successful exploitation could allow an attacker to impersonate an authenticated user and gain unauthorized access to device management functionality.	9.8	More Details
CVE-2026-	Xiiaozet LK100W exposes a critical management function that can be invoked without authentication, allowing a remote attacker to enable administrative services that should be restricted. Successful exploitation may permit	9.8	More Details

78239	unauthorized access to the device.		
CVE-2026-18431	The Avada theme for WordPress is vulnerable to Arbitrary File Write in all versions up to, and including, 7.16 when the Fusion Builder plugin is installed and active in versions up to, and including, 3.16. This is due to a chain of authorization and input validation weaknesses across the two components that makes it possible for unauthenticated attackers to write attacker-controlled files to the server. This can be used to create and execute arbitrary PHP files, resulting in remote code execution and complete site compromise. Successful exploitation requires both Avada and Fusion Builder to be installed and active, as well as certain administrator-authored content to be present.	9.8	More Details
CVE-2026-37003	Agno up to and including 2.5.8 is vulnerable to Remote Code Execution (RCE) via prompt injection. The PythonTools and ShellTools components pass unsanitized, LLM-generated arguments directly to execution sinks including exec(), runpy.run_path(), and subprocess.run(). An unauthenticated attacker can exploit this by embedding malicious instructions in content processed by the agent (such as web pages or documents), allowing for arbitrary code and OS command execution on the host server.	9.8	More Details
CVE-2026-82082	NUMail developed by Green-Computing has an OS Command Injection vulnerability. Unauthenticated remote attackers can inject arbitrary OS commands and execute them on the server.	9.8	More Details
CVE-2026-37006	A vulnerability in the WebSocket endpoint of gpt-researcher v0.14.7 and before allows an unauthenticated remote attacker to achieve code execution via malicious Model Context Protocol configurations.	9.8	More Details
CVE-2026-80600	In the Linux kernel, the following vulnerability has been resolved: batman-adv: dat: acquire ARP hw source only after skb realloc The pskb_may_pull() called by batadv_get_vid() could reallocate the buffer behind the skb. Variables which were pointing to the old buffer need to be reassigned to avoid an use-after-free.	9.8	More Details
CVE-2026-80609	In the Linux kernel, the following vulnerability has been resolved: qede: fix out-of-bounds check for cqe->len_list[] Move index check before element access.	9.8	More Details
CVE-2026-80612	In the Linux kernel, the following vulnerability has been resolved: net: lwtunnel: Drop skb metadata before LWT encapsulation skb metadata is meant for passing information between XDP and TC. It lives in the skb headroom, immediately before skb->data. LWT programs cannot access the __sk_buff->data_meta pseudo-pointer to metadata. However, LWT encapsulation prepends outer headers, moving skb->data back over the headroom where the metadata sits. On an RX-originated (forwarded) packet that still carries XDP metadata this goes wrong in two different ways, depending on the encap type: 1. Non-BPF LWT encaps (mpls, seg6, ioam6 ...) call skb_push()/skb_pull() and silently overwrite the metadata that sits in the headroom. 2) BPF LWT xmit calls bpf_skb_change_head(), which uses skb_data_move(). That helper expects metadata immediately before skb->data. But since the IP output path runs LWT xmit before neighbour output has built the outgoing L2 header, for forwarded packets skb->data points at the L3 header while skb_mac_header() still points at the old L2 header. skb_data_move() sees metadata ending at skb_mac_header(), not before skb->data, warns and clears metadata: WARNING: CPU: 21 PID: 454557 at include/linux/skbuff.h:4609 skb_data_move+0x47/0x90 CPU: 21 UID: 0 PID: 454557 Comm: napi/iconduit-g Tainted: G O 6.18.21 #1 RIP: 0010:skb_data_move+0x47/0x90 Call Trace: <IRQ> bpf_skb_change_head+0xe6/0x1a0 bpf_prog_...+0x213/0x2e3 run_lwt_bpf.isra.0+0x1d3/0x360 bpf_xmit+0x46/0xe0 lwtunnel_xmit+0xa1/0xf0 ip_finish_output2+0x1e7/0x5e0 ip_output+0x63/0x100 __netif_receive_skb_one_core+0x85/0xa0 process_backlog+0x9c/0x150 __napi_poll+0x2b/0x190 net_rx_action+0x40b/0x7f0 handle_softirqs+0xd2/0x270 do_softirq+0x3f/0x60 </IRQ> That is what happens, as for how to fix it - a received packet that carries metadata can reach an encap through any of the three LWT redirect modes: LWTUNNEL_STATE_INPUT_REDIRECT ip6_rcv_finish dst_input lwtunnel_input LWTUNNEL_STATE_OUTPUT_REDIRECT ip6_rcv_finish dst_input ip6_forward ip6_forward_finish dst_output lwtunnel_output LWTUNNEL_STATE_XMIT_REDIRECT ip6_rcv_finish dst_input ip6_forward ip6_forward_finish dst_output ip6_output ip6_finish_output ip6_finish_output2 lwtunnel_xmit Every encap funnels through the three LWT dispatch helpers, so drop the metadata there, right before handing the skb to the encap op. This single chokepoint covers all encap types and all three redirect modes: - lwtunnel_input(): seg6, rpl, ila, seg6_local - lwtunnel_output(): ioam6 - lwtunnel_xmit(): mpls, LWT BPF xmit Alternatively, we could clear the metadata right after TC ingress hook. That would require a compromise, however. Metadata would become inaccessible from TC egress (in setups where it actually reaches the hook it tact, that is without any L2 tunnels on path).	9.8	More Details
CVE-2026-80617	In the Linux kernel, the following vulnerability has been resolved: net: airoha: fix foe_check_time allocation size foe_check_time is declared as u16 pointer but was allocated with only ppe_num_entries bytes instead of ppe_num_entries * sizeof(u16). When airoha_ppe_foe_verify_entry() is called with hash >= ppe_num_entries/2, it writes beyond the allocated buffer, causing heap buffer overflow and potential kernel crash.	9.8	More Details
CVE-2026-76581	The WPMU DEV Dashboard plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 5.0.1. This is due to inconsistent and ambiguous HMAC message construction between the unauthenticated `wdpsso_step1` and `wdpsso_step2` AJAX actions, where step 1 signs and discloses an unseparated concatenation of the token, state, redirect, and domain values, while step 2 verifies an unseparated concatenation that omits the domain field. This makes it possible for unauthenticated attackers, on sites connected to WPMU DEV with Hub SSO enabled and mapped to an administrator, to obtain a valid HMAC from step 1 and replay it to step 2 by moving the domain value into the redirect field, resulting in an authenticated administrator session.	9.8	More Details

CVE-2026-19632	The TranslatePress – Translate Multilingual sites with AI Translation plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.3.1 via the 'trp_get_translations_regular' AJAX action. This makes it possible for unauthenticated attackers to extract the raw administrator password-reset URL — including the plaintext reset key and login parameters stored in the translation dictionary table — enabling full administrator account takeover. This vulnerability is only exploitable when automatic string saving is enabled (the default setting) and the target administrator's profile locale is set to a published secondary language, as these conditions cause the password-reset URL to be persisted as a translatable string in the secondary-language dictionary table.	9.8	More Details
CVE-2026-82266	Redpanda through 26.2.2 binds the Admin API to 0.0.0.0:9644 with admin_api_require_auth defaulting to false, treating unauthenticated requests as superusers. Attackers can reach port 9644 without credentials to create and delete broker accounts, modify cluster configuration, and disrupt partition replication.	9.8	More Details
CVE-2026-82860	@hulumi/policies versions before 1.3.2 fail to fully inspect inline and attached IAM policy evidence for the administrator-policy guardrail. Attackers can craft admin-equivalent policy paths that bypass policy evaluation controls.	9.8	More Details
CVE-2026-51674	Incorrect access control in the setScheduleCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to configure forced reboot tasks via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.8	More Details
CVE-2026-51693	Incorrect access control in the setVpnPassCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to weaken edge filtering via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.8	More Details
CVE-2026-51696	Incorrect access control in the setPortForwardRules function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to expose internal services via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.8	More Details
CVE-2026-51699	Incorrect access control in the setDmzCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to expose an internal host via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.8	More Details
CVE-2026-51708	Incorrect access control in the setWiFiWpsCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to change WPS availability via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.8	More Details
CVE-2026-51709	Incorrect access control in the setWiFiBasicCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to reconfigure primary Wi-Fi settings via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.8	More Details
CVE-2026-51715	Incorrect access control in the delMacFilterRules function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to remove MAC filter rules via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.8	More Details
CVE-2026-51718	Incorrect access control in the delStaticDhcpRules function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to remove static DHCP reservations via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.8	More Details
CVE-2026-73819	The affected Ebyte product's vendor configuration utility permits access to administrative functions without verifying the operator's identity under certain credential conditions. An unauthenticated attacker on the adjacent network could modify critical settings or change access credentials, potentially preventing legitimate administrators from managing the device.	9.8	More Details
CVE-2026-76133	The affected Ebyte product uses a deprecated hashing algorithm in an authentication-related operation. Under conditions where an attacker can manipulate or predict the authentication exchange, the weak construction may reduce the assurance provided by the authentication mechanism and facilitate unauthorized access.	9.8	More Details
CVE-2026-51724	Incorrect access control in the delSmartQosCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to remove Smart QoS rules via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.8	More Details
CVE-2026-51734	Incorrect access control in the informSlaveUpdate function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to trigger mesh slave update coordination via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.8	More Details
CVE-2026-51740	Incorrect access control in the killProcess function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to terminate critical services via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.8	More Details
CVE-2026-38577	Insecure hardcoded credentials in the Admin account of Tenda HG21 V4.0.0-260302 allows attackers to gain root access.	9.8	More Details
CVE-			

2026-79408	An OS command injection vulnerability in MetaGPT 0.8.1 allows an attacker to execute arbitrary commands via the path argument of RepoParser.rebuild_class_views() in metagpt/repo_parser.py.	9.8	More Details
CVE-2026-51670	Incorrect access control in the getSlaveUpdate function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to query slave upgrade status and affect upgrade bookkeeping via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.8	More Details
CVE-2026-82859	hulumi versions before v1.3.2 contain a deployment SCP template that allows tag-on-create bypasses for hulumi:iac-role protections. Attackers can bypass intended IAM boundary restrictions by exploiting the weakened SCP template in downstream deployments.	9.8	More Details
CVE-2026-82277	Argo Rollouts dashboard through 1.10.0 binds to all interfaces and exposes mutating Rollout operations without authentication, authorization, or CSRF protection. Attackers on the same network can invoke PromoteRollout, AbortRollout, RestartRollout, SetRolloutImage, UndoRollout, and RetryRollout operations across all namespaces accessible to the operator's kubeconfig.	9.8	More Details
CVE-2026-82858	@hulumi/drift versions before 1.3.2 accept externally supplied execute plans without sufficient provenance validation, allowing untrusted reconciliation input to be treated as trusted. Attackers can supply malicious execute plans that bypass security checks to perform unsafe reconciliation operations.	9.8	More Details
CVE-2026-82329	JFrog Artifactory contains an authentication weakness that, under default configuration, may allow an unauthenticated attacker with network access to obtain administrative privileges.	9.8	More Details
CVE-2026-19286	IBM Langflow OSS 1.0.0 through 1.11.1 could allow a remote attacker to execute arbitrary code due to improper enforcement of security restrictions on the A2A public endpoint.	9.8	More Details
CVE-2026-51663	Incorrect access control in the getWiFiApcliScan function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to trigger wireless scans and retrieve AP-client scan results via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.8	More Details
CVE-2026-16259	The Uix UserCenter WordPress plugin through 1.0.3 does not verify that the account being modified through an unauthenticated profile-update action belongs to the requester, and it authenticates that action with a token whose signing key is hardcoded and identical across every install, allowing unauthenticated attackers to forge a token for any user, overwrite an administrator's email and password, and take over the account.	9.8	More Details
CVE-2026-14494	The Sigma Forms Pro plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 1.4.5 via the handle_form_submission function. This is due to the plugin dynamically granting the unfiltered_upload capability to all users during form submissions and bypassing MIME type validation when allowed_file_types is not configured. This makes it possible for unauthenticated attackers to execute code on the server. Several default pre-built templates including Job Application, Support Ticket, and Wholesale Application have file upload fields with no file type restrictions configured by design, making this vulnerability immediately exploitable upon installation.	9.8	More Details
CVE-2026-82448	Shinobi before commit 5a76c74f contains a hardcoded connection key in the child node service that allows unauthenticated attackers to execute arbitrary database queries. Attackers reaching the child node port can present the hardcoded key during WebSocket handshake, then dispatch SQL queries through the onWebSocketDataFromChildNode handler to read and modify user records and camera configuration.	9.8	More Details
CVE-2026-82452	rust-iot-platform through commit 5df942ab contains an authentication bypass vulnerability where most REST API routes lack authentication guards in their handler signatures. Unauthenticated attackers can create, update, list, retrieve, and delete user accounts by directly accessing unprotected endpoints without providing valid credentials.	9.8	More Details
CVE-2026-19092	The Tutor LMS WordPress plugin before 4.0.6 does not prevent request data from overwriting internal variables while rendering templates, allowing unauthenticated users to invoke arbitrary zero-argument PHP functions and receive their output.	9.8	More Details
CVE-2026-15369	The Custom User Registration Fields for WooCommerce plugin for WordPress is vulnerable to Privilege Escalation in versions up to, and including, 2.2.3. This is due to the plugin accepting an attacker-controlled afreg_select_user_role value from the unauthenticated WooCommerce Store API /wc/store/v1/checkout request in the af_reg_checkout_data_to_order_meta_data_block() function, persisting it in order meta, and then passing it directly to WP_User::add_role() in the af_reg_custom_order_processing_function() function (hooked to woocommerce_thankyou) without validating against the plugin's admin-configured allowed role list. This makes it possible for unauthenticated attackers to elevate their privileges to Administrator by creating an account during checkout with a modified JSON body specifying administrator (or any other role slug) as the desired role. Note: The exploit requires the "User Role Selection" setting to be enabled.	9.8	More Details
CVE-2026-15980	The MyHome Core plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 4.4.5. This is due to missing authorization in the send_link() AJAX handler and improper token validation in the activate() function. This makes it possible for unauthenticated attackers to generate an activation token for an unconfirmed user account and obtain a valid authentication cookie for that account, including administrators. Successful exploitation requires the MyHome theme to be configured in legacy/WPBakery mode with frontend registration and confirmation email enabled, and the target account must not already have the	9.8	More Details

	myhome_agent_confirmed user meta set.		
CVE-2026-58574	Dell PowerStore contains a Missing Authentication for Critical Function vulnerability. An unauthenticated attacker with network access to the restricted management interface could potentially exploit this vulnerability to read internal system information from the appliance filesystem. This is a Critical vulnerability as it could expose sensitive information and credentials which allow full administrative access to the array.	9.8	More Details
CVE-2026-82854	Nodemailer before 8.0.4 is vulnerable to SMTP command injection through the unsanitized envelope.size parameter. When an application passes a custom envelope object with a size property containing CRLF characters to sendMail(), the value is concatenated into the SMTP MAIL FROM command (as SIZE=...) without sanitization, allowing injection of arbitrary SMTP commands such as RCPT TO to silently add attacker-controlled recipients. Exploitation requires the application to expose the envelope size to attacker-controlled input, as Nodemailer does not include size in the default auto-constructed envelope.	9.8	More Details
CVE-2026-82855	@hulumi/policies versions before 1.3.2 contain an evidence validation bypass vulnerability in Cloudflare and deployment-governance validators that allows attackers to suppress violations by submitting unrelated compliant evidence. Attackers can use evidence from different zones, hostnames, origins, or repositories to bypass security guardrails for unrelated resources in the same stack.	9.8	More Details
CVE-2026-82856	@hulumi/policies versions before 1.3.2 fail to properly validate set-qualified AWS IAM condition operators in GitHub OIDC trust policies. Attackers can use ForAnyValue:StringLike operators to hide wildcard GitHub Actions OIDC subject conditions from security guardrails.	9.8	More Details
CVE-2026-82857	hulumi versions before v1.3.2 contain a privilege escalation vulnerability in the weekly integration IAM policy that allows role lifecycle operations on af-e2e-* roles without sufficient boundary restrictions. Attackers with the documented principal can create persistent higher-privilege roles in the sandbox account.	9.8	More Details
CVE-2026-82460	Cloud Commander before 19.20.2 contains a directory traversal vulnerability in REST file-operation and markdown endpoints that fails to properly validate path normalization. Attackers can use path traversal sequences to read, write, move, or copy files outside the configured root directory.	9.8	More Details
CVE-2026-80630	In the Linux kernel, the following vulnerability has been resolved: net/sched: sch_fq_codel: Do not call qdisc_tree_reduce_backlog during peek before restoring qlen Whenever fq_codel drops packets during peek, it calls qdisc_tree_reduce_backlog. An issue arises because it calls qdisc_tree_reduce_backlog before it reincrements the qlen. If qlen drops to zero, but peek returns an skb, the parent's qlen_notify callback will be executed even though fq_codel still has 1 packet on the queue and, thus, will mistakenly deactivate the parent's class causing issues like a recent report [1] and a wild memory access in qfq: [29.371146][T360] Oops: general protection fault, probably for non-canonical address 0xfbd59c0000000024: 0000 [#1] SMP KASAN NOPTI [29.371666][T360] KASAN: maybe wild-memory-access in range [0xdead000000000120-0xdead000000000127] [29.371987][T360] CPU: 6 UID: 0 PID: 360 Comm: tc Not tainted 7.1.0-rc5-00285-gc530e5b2dbc6-dirty #82 PREEMPT(full) [29.372384][T360] Hardware name: Bochs Bochs, BIOS Bochs 01/01/2011 [29.372620][T360] RIP: 0010:qfq_deactivate_agg (include/linux/list.h:1029 (discriminator 2) include/linux/list.h:1043 (discriminator 2) net/sched/sch_qfq.c:1369 (discriminator 2) net/sched/sch_qfq.c:1395 (discriminator 2)) sch_qfq [29.373544][T360] RSP: 0018:ffff888102417370 EFLAGS: 00010216 [29.373800][T360] RAX: 0000000000000000 RBX: ffff88811224d568 RCX: dfffffc0000000000 [29.374079][T360] RDX: 1ffff11021fe1543 RSI: ffff88810ff0aa00 RDI: dfffffc0000000000 [29.374368][T360] RBP: ffff88811224c280 R08: dead000000000122 R09: 1bd5a00000000024 [29.374649][T360] R10: fffffbfff7940329 R11: fffffbfff7940329 R12: 0000000000000000 [29.374926][T360] R13: dead000000000100 R14: ffff88811224d580 R15: ffff88811224d578 [29.375207][T360] FS: 00007f5b794e5780(0000) GS:ffff88815d1e9000(0000) knlGS:0000000000000000 [29.375545][T360] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [29.375823][T360] CR2: 000055ffb091f000 CR3: 000000010a305000 CR4: 0000000000750ef0 [29.376103][T360] PKRU: 55555554 [29.376258][T360] Call Trace: [29.376401][T360] <TASK> ... [29.376885][T360] qfq_reset_qdisc (net/sched/sch_qfq.c:357 net/sched/sch_qfq.c:1487) sch_qfq [29.377074][T360] qdisc_reset (net/sched/sch_generic.c:1057) [29.377414][T360] __qdisc_destroy (net/sched/sch_generic.c:1096) [29.377600][T360] qdisc_graft (net/sched/sch_api.c:1062 net/sched/sch_api.c:1053 net/sched/sch_api.c:1159) [29.378593][T360] tc_get_qdisc (net/sched/sch_api.c:1528 net/sched/sch_api.c:1556) Fix this by only calling qdisc_tree_reduce_backlog in peek after the qlen is restored. [1] http://lore.kernel.org/netdev/CAN2cbVe79oj0O9==m4+4x3v+O+qzRagA=2=wkrp9i9=CqYvyZA@mail.gmail.com/	9.8	More Details
CVE-2026-81707	openssl_encrypt before 1.4.9 fails to sanitize the email field of imported identity documents, allowing attackers to inject ANSI escape sequences that forge the fingerprint verification line displayed to users. Attackers can deliver a crafted identity bundle through normal contact-exchange flows or keyserver responses to manipulate terminal output and display a fraudulent fingerprint, bypassing the out-of-band verification mechanism that protects against key substitution attacks.	9.8	More Details
CVE-2026-74744	In the Linux kernel, the following vulnerability has been resolved: ipvlan: inherit needed_headroom and needed_tailroom from phy_dev ipvlan devices inherit hard_header_len from phy_dev during ipvlan_init(), but leave needed_headroom and needed_tailroom set to 0. When the underlying phy_dev (or stacked lower device) requires extra headroom or tailroom for headers/trailers (e.g. macsec, ipsec, wireguard, tunnels, or veth with rx headroom), upper layers calculating packet headroom and tailroom fail to reserve sufficient space. This can result in reallocation overhead, skb headroom underflows, or KASAN slab-use-after-free crashes when dev_hard_header() / ipvlan_hard_header() prepends header data or when lower devices append tailroom. Fix this by: 1. Inheriting needed_headroom and needed_tailroom from phy_dev in ipvlan_init(). 2. Propagating needed_headroom and needed_tailroom updates to attached ipvlans in ipvlan_device_event() when receiving NETDEV_FEAT_CHANGE events.	9.8	More Details

CVE-2026-75338	disconf (Distributed Configuration Management Platform) 2.6.36 is vulnerable to Incorrect Access Control. The config-fetching APIs /api/config/item, /api/config/file, /api/config/list and /api/config/simple/list are exposed without authentication. The LoginInterceptor explicitly whitelists these four paths, so any anonymous attacker can read every configuration item and configuration file managed by the config center.	9.8	More Details
CVE-2026-74752	In the Linux kernel, the following vulnerability has been resolved: sctp: validate cookie AUTH state before use When cookie authentication is disabled, COOKIE_ECHO restores fixed-size AUTH fields directly from peer-controlled cookie bytes. A forged RANDOM length, HMAC list, or CHUNKS list can then reach association consumers with lengths or identifiers that were never validated against the local backing arrays. A forged RANDOM length can cause out-of-bounds reads during key-vector construction. A forged HMAC identifier also caused a 32-byte write past a zero-length AUTH chunk, providing a primitive for a local privilege escalation chain. Validate the cookie's RANDOM, HMACS, and CHUNKS parameters at the cookie trust boundary before copying them into the association. Reject invalid types, malformed lengths, unsupported HMAC identifiers, HMAC lists without SHA1, and forbidden chunk ids.	9.8	More Details
CVE-2026-75330	The front-end interface /superdiamond/preview/{projectCode}/{module}/{type} of super-diamond-server <= 1.3.3 is vulnerable to SQL injection. The module parameter is directly concatenated into the SQL IN clause through StringUtils.split() and string concatenation without being parameterized and bound.	9.8	More Details
CVE-2026-75329	The Netty configuration distribution service (port 8283) of super-diamond-server <= 1.3.3 has no authentication mechanism. Attackers can directly obtain the full configuration of any project (including database passwords, API keys, etc.) by sending a TCP request without any credential.	9.8	More Details
CVE-2026-80519	In the Linux kernel, the following vulnerability has been resolved: ovpn: finish crypto callback cleanup before peer release Crypto completion callbacks hold both key-slot and peer references. The peer reference pins the netdev, and dropping the last peer reference can let netdev unregistration and module removal make progress. Do not release that peer reference before the callback has finished its own cleanup. If ovpn_crypto_key_slot_put runs after ovpn_peer_put, it can schedule an RCU callback backed by module text after ovpn_cleanup rcu_barrier has already run. The TX error path also freed the remaining skb after ovpn_peer_put, leaving callback cleanup outside the peer/netdev lifetime window. Release the key slot and free any remaining skb first, then drop the peer reference as the last callback action.	9.8	More Details
CVE-2026-80528	In the Linux kernel, the following vulnerability has been resolved: ceph: avoid fs reclaim while using current->journal_info handle_reply() stores a `ceph_mds_request` pointer in `current->journal_info` while filling the inode and dentry cache from an MDS reply. An allocation in this section can enter direct reclaim and prune dentries from another filesystem. If this dirties an ext4 inode, ext4 starts a JBD2 transaction. JBD2 interprets the Ceph request in `current->journal_info` as a journal handle and dereferences the request's `r_tid` as `h_transaction`, causing a kernel crash, e.g.: Unable to handle kernel paging request at virtual address 00000000077b4818 [...] Internal error: Oops: 0000000096000004 [#1] SMP Modules linked in: CPU: 6 UID: 0 PID: 2699135 Comm: kworker/6:3 Tainted: G W 6.18.38-i3 #1113 NONE [...] Workqueue: ceph-msgr ceph_con_workfn pstate: 80400009 (Nzcv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : jbd2__journal_start+0x2c/0x208 lr : __ext4_journal_start_sb+0x100/0x178 [...] Call trace: jbd2__journal_start+0x2c/0x208 (P) __ext4_journal_start_sb+0x100/0x178 ext4_dirty_inode+0x3c/0x90 __mark_inode_dirty+0x58/0x400 iput.part.0+0x2b0/0x370 iput+0x18/0x30 dentry_unlink_inode+0xc0/0x158 __dentry_kill+0x80/0x250 shrink_dentry_list+0x90/0x130 prune_dcache_sb+0x60/0x98 super_cache_scan+0xe8/0x190 do_shrink_slab+0x174/0x388 shrink_slab+0xd8/0x4c0 shrink_node+0x31c/0x908 do_try_to_free_pages+0xd0/0x508 try_to_free_pages+0x11c/0x238 __alloc_frozen_pages_noprof+0x4d0/0xdd0 __folio_alloc_noprof+0x18/0x70 __filemap_get_folio+0x248/0x440 ceph_readdir_prepopulate+0x570/0x9e8 mds_dispatch+0x1424/0x1ba0 ceph_con_process_message+0x74/0xa0 ceph_con_v1_try_read+0x3a0/0x1510 ceph_con_workfn+0x260/0x460 Enter a scoped NOFS allocation context and leave it after clearing `journal_info`. This prevents filesystem reclaim from recursing into another filesystem while the field contains Ceph-private data.	9.8	More Details
CVE-2026-80557	In the Linux kernel, the following vulnerability has been resolved: libceph: fix OOB read in decode_watchers() via missing bounds check ceph_start_decoding() validates that struct_len bytes remain in the buffer after the encoding header, but accepts struct_len=0 as valid: ceph_decode_need(p, end, 0, bad) always passes. When a malicious or compromised OSD sends an obj_list_watch_response_t reply with struct_len=0, ceph_start_decoding() returns success with p == end, leaving zero bytes guaranteed for subsequent reads. The immediately following ceph_decode_32(p) in decode_watchers() has no preceding bounds check. With p == end this is a 4-byte read past the validated buffer boundary. The garbage value is then passed directly to kzalloc_objs() as the watcher count. The sibling function decode_watcher() already uses the safe variants (ceph_decode_copy_safe, ceph_decode_64_safe, ceph_decode_skip_32) after its own ceph_start_decoding() call. decode_watchers() is the only site that uses the bare variant, confirming an oversight. Fix by replacing ceph_decode_32(p) with ceph_decode_32_safe(p, end, *num_watchers, bad), consistent with the established pattern. Attacker model: a malicious or compromised OSD in a multi-tenant Ceph deployment (e.g. cloud) can trigger this against any kernel client that calls CEPH_OSD_OP_LIST_WATCHERS, without any further privileges beyond OSD session establishment. [idryomov: trim changelog]	9.8	More Details
CVE-2026-	In the Linux kernel, the following vulnerability has been resolved: libceph: Avoid using invalid osd indices from primary_temp A corrupted osdmap received from a Ceph monitor or OSD may contain osd indices in its pg_temp, primary_temp, pg_upmap, and pg_upmap_items parts that don't exist, i.e., that are greater than max_osd or smaller than CEPH_HOMELESS_OSD (-1). These indices are used to create the up and acting set in ceph_pg_to_up_acting_osds(), called from calc_target(). While most of these osd indices are checked, the one from primary_temp is not. Subsequently, this may lead to calc_target() returning this (potentially invalid) index as	9.8	More

80558	target osd for a (linger) request. Because the osd_state, osd_weight, and osd_addr arrays only contain max_osd entries (with indices 0 to max_osd -1), this leads to out-of-bounds accesses when trying to read values from these arrays. This patch fixes the issue by adding a check to get_temp_osds(), so that only valid osd indices from primary_temp are used, and it falls back to using the primary from pg_temp or the up set if it is invalid. [idryomov: changelog]		Details
CVE-2026-75414	In AntFlow V2.0.0, ActivitiTest.java enables users to execute JUEL expressions without filtering the user input, which leads to a command execution vulnerability.	9.8	More Details
CVE-2026-80561	In the Linux kernel, the following vulnerability has been resolved: libceph: fix multiple unsafe decodes in decode_locker() decode_locker() in cls_lock_client.c contains three unsafe decode operations that allow a malicious or compromised OSD to trigger slab-out-of-bounds reads: 1. ceph_decode_copy() at the locker_id_t name field has no preceding bounds check. With p == end after ceph_start_decoding() accepts struct_len=0, this reads sizeof(ceph_entity_name) = 9 bytes past the validated buffer boundary. 2. *p += sizeof(struct ceph_timespec) after the locker_info_t header is an unchecked pointer advance. A malicious OSD can position p past end, causing all subsequent _safe checks to pass against a bogus boundary. 3. len = ceph_decode_32(p) has no preceding bounds check, and the immediately following *p += len is uncapped. A malicious OSD can send len=0xffffffff, advancing p gigabytes past end and escaping the decode window entirely. Fix all three by replacing bare operations with their safe variants: ceph_decode_copy -> ceph_decode_copy_safe *p += sizeof(...) -> ceph_decode_skip_n ceph_decode_32(p) -> ceph_decode_32_safe *p += len -> ceph_decode_skip_n A new label is added to return -EINVAL on any bounds violation. -EINVAL is appropriate here: the data received from the OSD is structurally malformed, which is an invalid argument to the decode contract regardless of whether the caller or the wire is at fault. Attacker model: a malicious or compromised OSD in a multi-tenant Ceph deployment can trigger this against any kernel client that issues the lock.get_info class method (e.g. during RBD exclusive lock acquisition) without any further privileges beyond OSD session establishment. [idryomov: use ceph_decode_skip_string() to skip description, trim changelog]	9.8	More Details
CVE-2026-80586	In the Linux kernel, the following vulnerability has been resolved: mptcp: options: reset DSS fields in case of unexpected size A remote peer could send a malformed DSS with a wrong size, followed by another DSS or MPC + Data. In this case, the first suboption will be ignored, but leaving some fields written, which could lead to inconsistency or access uninitialized data. Explicitly reset the fields that could have been modified in case of unexpected size.	9.8	More Details
CVE-2026-80587	In the Linux kernel, the following vulnerability has been resolved: mptcp: avoid combining some incoming suboptions Some MPTCP suboptions are mutually exclusive according to the RFC8684, but also because in different places, the code doesn't expect some combinations to be present. That's specially true for suboptions that would be present twice, but with different attributes. The new restrictions are the same as the ones applied on the output side, with mptcp_write_options. The same rules can be reused with a small fix: an MP_FASTCLOSE can be used with a DSS when the sender picks this option [1], which is not the case on Linux. Here are the rules: Which options can be used together? X: mutually exclusive O: often used together C: can be used together in some cases P: could be used together but we prefer not to (optimisations) | Opt: | MPC | MPJ | DSS | ADD | RM | PRIO | FAIL | FC | |------|------|------|------|------|------|------|------| | MPC |------|------|------|------|------|------|------|------| | MPJ | X |------|------|------|------|------|------|------| | DSS | X | X |------|------|------|------|------|------| | ADD | X | X | P |------|------|------|------|------|------| | RM | C | C | C | P |------|------|------|------| | PRIO | X | C | C | C | C |------|------|------| | FAIL | X | X | C | X | X | X |------|------| | FC | X | X | P | X | X | X | X |------| | RST | X | X | X | X | X | X | O | O | |------|------|------|------|------|------|------|------|------| The only difference is with the 'P': another stack could send and ADD_ADDR with other suboptions (DSS, RM_ADDR), and this should be allowed. A few points of attention: - In theory, an MP_CAPABLE could be used with a RM_ADDR, but there is no reason to add it with a SYN. Note that even with a 4th ACK, it doesn't seem to be useful, except when IDs are known in advance via another channel. Better not to break that. - Now, combining both an MP_CAPABLE and an MP_JOIN will no longer result to a reject of the two options, but only the second suboption is ignored. That seems OK to do that for this unexpected error. At least now all inconsistent combinations are handled the same way. This could change later in next. This also means the explicit checks for having both MPC + MPJ in subflow.c will now be unreachable. That's fine, they will be removed in a follow-up patch. - In case of conflicting combinations, the extra suboption(s) is/are ignored: having such combinations either means the remote peer is buggy, or is evil. The simplest action is then taken in this case: stop processing the current suboption. - In mp_opt->suboptions, there is also a bit reserved to the checksum, which can be used in an MP_CAPABLE and a DSS. Each time a DSS option can be used in parallel with another option, the checksum can be set, so the verification is combined into a new OPTIONS_MPTCP_DSS macro. - An MP_CAPABLE ACK can carry a Data-Level Length, and an optional Checksum: they are the same as the ones found in a DSS, because a DSS cannot be used in parallel to an MP_CAPABLE. Similarly, even if there is room, a DSS cannot be used with an MP_JOIN.	9.8	More Details
CVE-2026-75411	JeecgBoot v3.9.2 is vulnerable to Remote command execution. The CodeNode component of the AI Flow module supports Groovy script execution. While the `SecurityCheck` class employs a blacklist mechanism to intercept dangerous calls, the dynamic nature of Groovy allows this blacklist to be completely bypassed through string concatenation and reflection.	9.8	More Details
	In the Linux kernel, the following vulnerability has been resolved: block: stop the timeout timer when releasing a never added disk disk_release() undoes blk_mq_init_allocated_queue() for a disk whose probe failed before add_disk(), but it only calls blk_mq_exit_queue(). Nothing there stops q->timeout, and that timer rolls forward: it stays pending until it next expires, not until the last request completes. So if the driver issued any I/O before adding the disk, the request_queue is freed while still linked into a timer wheel bucket. Commit 6f8191fdf41d		

CVE-2026-80589	("block: simplify disk shutdown") dropped the blk_cleanup_queue() call that used to stop it. __del_gendisk() and blk_mq_destroy_queue() still do; only the probe failure path lost it. nvme gets there because nvme_update_ns_info() submits Report Zones or FDP io-mgmt-recv on ns->queue before the disk is added, so a later failure - a concurrent reset setting NVME_CTRL_FROZEN, or device_add_disk() failing - lands in put_disk() with the timer armed: BUG: KASAN: slab-use-after-free in detach_if_pending+0x30c/0x340 Write of size 8 at addr ffff888004d71310 by task kworker/u8:2/37 __timer_delete_sync+0x156/0x240 kernel/time/timer.c:1621 blk_sync_queue+0x22/0x40 block/blk-core.c:222 nvme_sync_queues+0x100/0x150 drivers/nvme/host/core.c:5362 nvme_reset_work+0x138/0x930 drivers/nvme/host/pci.c:3264 Allocated by task 34: __blk_mq_alloc_disk+0x33/0x100 block/blk-mq.c:4462 nvme_alloc_ns+0x290/0x3870 drivers/nvme/host/core.c:4146 Freed by task 0: blk_free_queue_rcu+0x3a/0x50 block/blk-core.c:254 rcu_core+0xc10/0x1730 kernel/rcu/tree.c:2857 The queue being synced there is ctrl->admin_q, only a victim sharing a timer wheel bucket with the freed queue's dangling entry; other runs tripped in enqueue_timer(), __run_timers() or blk_mq_timeout_work(). Failing nvme_alloc_ns() with a debug patch makes it deterministic: one leaked timer trips KASAN within seconds, while 1987 patched releases produced no splat. Stop the timer and the queue work items before blk_mq_exit_queue(), like blk_mq_destroy_queue() does. Found by FuzzNvme.	9.8	More Details
CVE-2026-54569	SENAITE.CORE is the core framework for the SENAITE laboratory information management system. From 2.0.0 to 2.6.0, the SENAITE.CORE JSON API permits unauthenticated remote code execution through a two-request chain involving missing authorization and unsafe evaluation. The state-changing routes in src/bika/lims/jsonapi/update.py, including update, update_many, remove, doActionFor, doActionFor_many, and getusers, do not enforce the senaite.core: Access JSON API permission before resolving attacker-selected objects. In src/bika/lims/jsonapi/init.py, set_fields_from_request passes raw request values for RecordsField and RecordField instances to eval() before field mutator write-permission checks execute. An anonymous attacker can discover the bika_setup object identifier through @@uuid, send a value such as RejectionReasons to /@@API/update, and execute arbitrary Python in the Zope worker before a later mutation failure rolls back ZODB changes. The same unsafe evaluation pattern is present in src/senaite/core/browser/fields/record.py and src/senaite/core/browser/fields/records.py. Successful exploitation can expose or modify laboratory data, files, and accounts and can disrupt the service.	9.8	More Details
CVE-2026-80428	ILIAS deserialises stored session data for an unauthenticated caller. The Shibboleth back-channel endpoint at components/ILIAS/AuthShibboleth/resources/shib_logout.php runs in a context that ilInitialisation exempts from authentication, and its logout-notification handler locates the session to terminate by reading every live row of the session table and passing each row's stored data to a hand-written parser that calls unserialize without restricting which classes may be constructed. Any serialised object present in any session row is therefore instantiated on behalf of an anonymous request, and object destructors run when those objects are discarded. A serialised object can be placed into a session row without logging in, because the LTI authentication entry point stores request parameters into the session and is reachable on a path the same initialisation code exempts from authentication. A class bundled with the application writes a JSON-encoded structure to a file named by one of its own properties when it is destroyed, which places attacker-controlled content at an attacker-chosen path below the web root and results in code execution as the web server user. Versions 9.22, 10.10 and 11.3 remove the endpoint's logout-notification implementation.	9.8	More Details
CVE-2026-52103	A zero-click remote code execution (RCE) vulnerability in the /Terminal/Notification.hs component of SimpleX Chat before v6.5 allows attackers to execute arbitrary commands in the context of the application without user interaction via sending a crafted payload in a text message.	9.8	More Details
CVE-2026-81032	NebulaGraph exposes its runtime configuration over an unauthenticated HTTP service. Each daemon starts the web service defined in src/webservice/WebService.cpp, whose bind address defaults to all interfaces, and registers routes for reading and writing gflags alongside status and statistics. Neither the service nor its router carries any authentication, token check or address restriction. The read route returns the daemon's full set of runtime flag values, which includes the configured certificate, key and certificate-authority paths, the password file path, data directories and the transport-security enable flags. The write route parses a supplied map and applies each entry through the gflags runtime setter, so a caller able to reach the port can change the daemon's behaviour without restarting it, including disabling the transport-security flags, redirecting log files and altering flags such as failed_login_attempts and password_lock_time_in_secs. Public reports of this endpoint describe a single name, enable_authorize, being refused by the handler; at release 3.8.0 that refusal is not present and the handler applies every name it is given.	9.8	More Details
CVE-2026-75334	The report module in the backend of smart-web2 v1.3.1 is vulnerable to arbitrary SQL execution. The sqlResource.sql parameter is stored in the t_report_sql_resource table through the ReportController.save() interface and directly embedded into Hibernate native queries without any parameterization or filtering.	9.8	More Details
CVE-2026-75327	In DocSys-master V2.02.85, the uploadMarkdownPic interface in src/com/DocSystem/controller/DocController.java has an arbitrary file upload vulnerability:	9.8	More Details
CVE-2026-68000	The front-end interface /cms/category/list of MCMS <=6.2.0 is vulnerable to SQL injection. The size parameter is directly concatenated into the LIMIT clause of SQL through FreeMarker ${size} without being parameterized and bound. The built-in SqlInjectionUtil employs regular expression blacklist filtering, yet keywords like CREATE/TABLE/SET/PREPARE/EXECUTE are not included in the list, allowing for bypassing. Attackers can execute stacked SQL statements without logging in.	9.8	More Details
CVE-2026-	Gitea before 1.27.1 allows remote code execution via the diffpatch API through Git hook installation.	9.8	More

60004			Details
CVE-2026-26448	Stomper 5e2741e is vulnerable to Use-After-Free. When a client sends multiple CONNECT frames on the same TCP connection, and subsequently another client (or a later connection) sends SEND frames to a destination previously subscribed on that connection, the broker may dereference a pointer to a StompStreamSocket object that has already been freed. This results in a heap use-after-free and process crash. Because the protocol does not authenticate or restrict such sequences by default.	9.8	More Details
CVE-2025-70293	An issue was discovered in Denx U-Boot before 2026.04. An integer overflow vulnerability exists in function ext4fs_get_bgdtable, the size calculation can lead to under allocation and this underallocated buffer will be used in memcpy() which could lead to arbitrary code execution, a denial of service, or other unspecified impacts.	9.8	More Details
CVE-2025-70290	An issue was discovered in Denx U-Boot before 2026.04. An integer overflow vulnerability in the ZFS filesystem support can be triggered by malformed on-disk metadata. The issue may result in incorrect memory allocation followed by out-of-bounds memory access, potentially leading to a crash or arbitrary code execution during the boot process.	9.8	More Details
CVE-2023-42179	Bird Home Automation GmbH D1101V-F 000140 is vulnerable to Incorrect Access Control via the Key derivation process, password validation process.	9.8	More Details
CVE-2026-81702	openssl_encrypt before 1.4.9 fails to re-derive and validate fingerprints when loading identities from identity.json, allowing attackers to substitute public keys in identity stores. Attackers can replace legitimate public keys with their own while maintaining the claimed fingerprint, enabling silent key substitution where encryption uses attacker keys and signature verification appears valid.	9.8	More Details
CVE-2026-75325	DWSurvey v6.14.0 is is vulnerable to authentication bypass via the '/api/dwsurvey/none/' and '/api/dwsurvey/up/**' parameters.	9.8	More Details
CVE-2025-61163	Cohere North AI v1.1.5 was discovered to contain excessively permissive cross-domain policy with untrusted domains. This occurs via the server failing to validate the Origin header of incoming connection requests.	9.8	More Details
CVE-2026-74746	In the Linux kernel, the following vulnerability has been resolved: netfilter: flowtable: publish GC-visible tuple last nf_flow_table_iterate() only treats original-direction tuple nodes as owning entries. Publishing the original node first lets GC observe and free a flow while flow_offload_add() is still inserting the reply node. Publish the reply node first and the original node last so GC never sees a partially installed flow. KASAN can trigger slab-use-after-free read and write reports in the flowtable/rhashtable path (rht_deferred_worker, jhash, flow_offload_del, flow_offload_lookup, etc.).	9.8	More Details
CVE-2026-75336	Funiture 1.0.0 is vulnerable to SQL Injection in the backend tool interfaces /sys/tool/select.json and /sys/tool/update.json.	9.8	More Details
CVE-2026-47884	Use of XsltView in a Spring MVC application can result in SSRF and RCE attack if the application has an "/**" mapping that results in view rendering, and where the view name is not explicitly specified. Spring Framework 7.0.0 - 7.0.8 Spring Framework 6.2.0 - 6.2.19 Spring Framework 6.1.0 - 6.1.28 Spring Framework 6.0.0 - 6.0.30 Spring Framework 5.3.0 - 5.3.49 Spring Framework 5.2.25.RELEASE and earlier	9.8	More Details
CVE-2026-80203	The getgrav/grav-plugin-api plugin before 1.0.18 does not enforce API-key scope in the requireNotSuperTarget() function in UsersController.php across seven sensitive user-management endpoints. The check uses isSuperAdmin() on the acting account rather than verifying whether the specific API key carries super authority (via isSuperWithinScope()). As a result, an API key scoped below full super authority but belonging to a super-admin account can act against other super-admin accounts—disabling their 2FA, deleting their avatar, minting new API keys under their identity, or deleting their existing API keys.	9.8	More Details
CVE-2026-81701	openssl_encrypt versions before 1.4.9 use a denylist to identify trusted built-in plugins, allowing unsigned plugins in top-level plugins/ directories and unknown subdirectories to bypass signature verification. Attackers can place malicious unsigned plugins following documented installation paths to achieve arbitrary code execution in the CLI process with access to passwords and cryptographic keys.	9.8	More Details
CVE-2026-81700	openssl_encrypt versions before 1.4.9 contain a signature verification vulnerability in gpg_runner.verify_detached that accepts revoked and expired keys by only checking VALIDSIG status without inspecting REVKEYSIG, EXPKEYSIG, or gpg exit codes. Attackers holding compromised-then-revoked signing keys or expired project keys can bypass signature verification to execute malicious plugins in the host process.	9.8	More Details
CVE-2026-75357	An issue in Bilibili Desktop v.1.17.9 allows a remote attacker to execute arbitrary code via the bili-inject.js and bili-bridge.js components.	9.8	More Details
CVE-2026-80235	EFence developed by Thinking Software Technology has an Arbitrary File Upload vulnerability. Unauthenticated remote attackers can upload and execute web shell backdoors, thereby enabling arbitrary code execution on the server.	9.8	More Details

CVE-2026-59683	The OpenRGB network protocol allows to write attacker controlled strings into arbitrary file system paths (extension of CVE-2026-59682). This allows either a full system compromise from local or remote (if the daemon is running as root) or a full account takeover (if the daemon is running in user context).	9.8	More Details
CVE-2026-26897	An issue in EcoOnline EHS (com.airsweb.v10) application for Android, version 0.2.499 allows a remote attacker to obtain sensitive information and execute arbitrary code via the AndroidManifest.xml component	9.8	More Details
CVE-2026-80349	TarsWeb decides whether a request comes from a trusted local caller using a client-controlled header. app.js sets Koa's proxy option to true without naming which upstream proxies may be trusted and without limiting the number of forwarded hops, so the request address Koa reports is taken from the X-Forwarded-For header supplied by the caller. In midware/ssoMidware.js a single branch covers both the ignored-path list and the ignoreIps allowlist from config/loginConf.js, which contains the loopback address, and that branch assigns the effective account identity from the uid query parameter before falling through to the request without validating any ticket, cookie or password. A request carrying a forged X-Forwarded-For value naming the loopback address and a uid naming an existing account therefore reaches every route the console mounts as that account, including an administrator, with no credential of any kind. Those routes include user and role administration, service configuration, and package upload and deployment. Version 3.0.16 separates the two branches so that a match on the address allowlist assigns the configured default account rather than one named by the caller.	9.8	More Details
CVE-2026-74233	Zbtlink WE1326, WE357, WE5926, WE5926-WD, WE826-Q, WE826-T2, WE826-WD, WG108, and WG3526 firmware 19.1101, Zbtlink WE2426-C firmware 19.1112, Zbtlink WE5926-EC_QP firmware 20.0516, Zbtlink WF3526-P firmware 19.051, CTN720-W1, LF-1541, and MT7620N firmware 19.1101, and WRC1 firmware 20.0622 contain an unauthenticated command injection in the infosrvd service (UDP/9992). A remote unauthenticated attacker can send a crafted UDP packet to execute arbitrary commands as root. The service's authentication uses a hardcoded salt and an all-zero wildcard MAC bypass, rendering it ineffective.	9.8	More Details
CVE-2026-74232	Zbtlink L3_V2_8 firmware 3.0.0.4.528, Zbtlink WE826-T2 firmware 19.1101, Zbtlink ZBT-7628 firmware 1.0.0.2.007, Zbtlink ZBT-ZBT7621 firmware 1.0.0.3.001, MoreQuick MQAC-7620, MQAC-7620A, MQAP-7620, MQAP-7620A, and MQAP-7628 firmware 1.0.0.2.000, AP522 firmware 1.0.0.2.014, AP7628 and HC5661A firmware 3.0.0.4.380, APG721B firmware 19.0809, HK300 firmware 1.0.0.2.032, and MAP-N10 firmware 1.0.0.2.044 ship a backdoor command-and-control implant (yunmgrd) reachable over an unauthenticated cleartext UDP channel to a hardcoded C2 server. A remote unauthenticated attacker on the network path can hijack the channel and execute arbitrary commands as root. The attacker can also modify DNS entries, exfiltrate PPPoE credentials, and open reverse SSH tunnels.	9.8	More Details
CVE-2026-78292	Unauthenticated PHP Object Injection in Hash Form <= 1.4.1 versions.	9.8	More Details
CVE-2026-18080	The ERP: Complete HR, Accounting & CRM Suite Built for WooCommerce plugin for WordPress is vulnerable to Unrestricted File Type Upload in all versions up to, and including, 1.17.8 via the save_attachments() function. This is due to missing file extension validation and missing path normalization when CRM Email Connect processes inbound IMAP email attachments. This makes it possible for unauthenticated attackers to send a crafted email to the site's configured inbound mailbox with a forged References header matching the plugin's expected pattern and an attachment filename such as `../helper.php`, causing the cron-based IMAP sync job to write attacker-controlled PHP outside of the .htaccess-protected `crm-attachments` directory and into `wp-content/uploads/`. On configurations where PHP executes in uploads, this can lead to remote code execution. Exploitation requires the CRM module and IMAP Email Connect feature to be enabled and configured.	9.8	More Details
CVE-2026-78286	Unauthenticated PHP Object Injection in Geo Controller <= 8.9.8 versions.	9.8	More Details
CVE-2026-47890	Spring MVC and WebFlux applications are vulnerable to stream corruption when using Server-Sent Events (SSE) with view fragments. Spring Framework 7.0.0 - 7.0.8 Spring Framework 6.2.0 - 6.2.19	9.8	More Details
CVE-2026-77557	A malicious actor with access to the network could exploit an Improper Access Control vulnerability found in UniFi Protect AI Key to escalate privileges on the device.	9.8	More Details
CVE-2026-77552	A malicious actor with access to the network could exploit an Improper Input Validation vulnerability found in UniFi Enterprise Audio/Video Bridge to execute a Command Injection on the device.	9.8	More Details
CVE-2026-47892	A WebFlux application using functional endpoints and deployed with DispatcherServlet may be vulnerable to a header predicate bypass in a pre-flight request. Spring Framework 7.0.0 - 7.0.8 Spring Framework 6.2.0 - 6.2.19 Spring Framework 6.1.0 - 6.1.28 Spring Framework 6.0.0 - 6.0.30 Spring Framework 5.3.0 - 5.3.49 Spring Framework 5.2.5.RELEASE - 5.2.25.RELEASE	9.8	More Details
CVE-2026-	A Spring WebFlux application that relies on the Aalto XML processor to parse XML input does not correctly enforce the maxInMemorySize limit. Spring Framework 7.0.0 - 7.0.8 Spring Framework 6.2.0 - 6.2.19 Spring Framework 6.1.0 - 6.1.28 Spring Framework 6.0.0 - 6.0.30 Spring Framework 5.3.0 - 5.3.49 Spring Framework 5.2.25.RELEASE	9.8	More Details

47891	and earlier		
CVE-2026-74743	In the Linux kernel, the following vulnerability has been resolved: macvlan: inherit needed_headroom and needed_tailroom from lowerdev macvlan devices inherit hard_header_len from lowerdev during macvlan_init(), but leave needed_headroom and needed_tailroom set to 0. When the underlying lowerdev requires extra headroom or tailroom for headers/trailers (e.g. macsec, ipsec, wireguard, tunnels, or veth with rx headroom), upper layers calculating packet headroom and tailroom fail to reserve sufficient space. This can result in reallocation overhead, skb headroom underflows, or KASAN slab-use-after-free crashes when dev_hard_header() / macvlan_hard_header() prepends header data or when lower devices append tailroom. Fix this by: 1. Inheriting needed_headroom and needed_tailroom from lowerdev in macvlan_init(). 2. Propagating needed_headroom and needed_tailroom updates to attached macvlans in macvlan_device_event() when receiving NETDEV_FEAT_CHANGE events.	9.8	More Details
CVE-2026-74737	In the Linux kernel, the following vulnerability has been resolved: net: ethernet: ti: am65-cpsw-nuss: Fix port_id extraction from SRC TAG On the packet reception path, the ID of the MAC Port on which the packet was received, is embedded in the RX DMA Descriptor's metadata. The ID is extracted using the helper function cppi5_desc_get_tags_ids() which fills in the 16-bit Source Tag into the 'port_id' variable. However, it is only the lower 8-bits of the 16-bit Source Tag that represent the MAC Port ID, while the upper 8-bits are Hardware-Reserved and carry an arbitrary value. With the existing logic, sporadic kernel crash is observed due to the subsequent driver code accessing out-of-bound memory because of an invalid port_id. Hence, fix the port_id extraction logic to use only the lower 8-bits of the Source Tag as the MAC Port ID.	9.8	More Details
CVE-2025-61165	An arbitrary file upload vulnerability in the /v1/my_drive/batch_upload component of cohere North AI v1.1.5 allows attackers to exeute arbitrary code via uploading a crafted file.	9.8	More Details
CVE-2026-32566	Unauthenticated Privilege Escalation in ACPT (Pro) - Custom Post Types Plugin for WordPress <= 2.0.63 versions.	9.8	More Details
CVE-2026-54754	Klever-Go is the Go implementation of the Klever blockchain protocol. Prior to 1.7.19, marketplace settlement in core/kapp/market/market.go reads MarketOrderData.ReferralPercentage from the listing while reading asset.Royalties.MarketPercentage live at purchase time. An asset owner can create a valid listing and then use AssetTrigger UpdateRoyalties to make the combined referral and royalty percentages exceed the bid. executeBuyMarket pays referral and royalty amounts unconditionally while computeMarketOwnerAmount silently skips a nonpositive seller remainder, allowing MarketBuy, BuyItNow, or auction Claim settlement to credit more KLV or sale currency than the buyer paid. This can create unbacked currency and corrupt token supply integrity. This issue is fixed in version 1.7.19.	9.6	More Details
CVE-2026-54755	Klever-Go is the Go implementation of the Klever blockchain protocol. Prior to 1.7.19, split-royalty fields decoded in core/kapp/builtInFunctions/utils.go can contain values greater than core.HundredPercent, and core/kapp/kda/create.go and core/kapp/kda/trigger.go sum those values in uint32 accumulators. Crafted values such as two 0x80000000 entries wrap the validation sum to zero and pass CheckValid100Params. Royalty payout paths in core/kapp/accounts/accounts.go, core/kapp/market/market.go, and core/kapp/ito/ito.go then credit each oversized split amount and silently discard a negative remainder, allowing ordinary asset transfers, marketplace purchases, or ITO purchases to create unbacked KLV or other assets. This issue is fixed in version 1.7.19.	9.6	More Details
CVE-2026-49003	Attackers can exploit command injection vulnerabilities to delete core system runtime files, causing the monitoring module to crash and become paralyzed; simultaneously, they can obtain root privileges to steal configuration passwords such as SNMP, thereby tampering with critical system parameters and triggering abnormal operation of the entire power system.	9.6	More Details
CVE-2026-82870	ToolJet before v3.16.208 fails to validate organizationId ownership in database write and destroy routes, allowing any builder-role user to create, alter, or drop tables in other organizations' databases. Attackers can exploit missing organization-resolving guards to permanently delete tables, insert arbitrary data, and modify schemas across tenant boundaries on shared instances.	9.6	More Details
CVE-2026-53552	Goploy is an open-source automation deployment system. In versions 1.17.5 and prior, Project.AddFile, Project.EditFile, Project.RemoveFile, and Project.Edit in cmd/server/api/project/handler.go accept a project or project-file row id from the JSON body and act on it without checking that the project belongs to the caller's namespace. The corresponding model.ProjectFile.GetData and model.Project.GetData queries filter only by row id. A user holding the manager role (or any role that includes the FileSync / EditProject permission) in their own namespace can read, write, or delete files in any project across the install, and can rewrite any project's git remote URL by submitting the foreign id in the body. The git-URL primitive escalates to RCE on the next deploy because Edit runs git remote set-url on the project's working tree. At time of publication, there are no known publicly available patches.	9.6	More Details
CVE-2026-54523	Kyverno is a policy engine designed for cloud native platform engineering teams. From 1.18.0 until 1.18.2, the NamespacedMutatingPolicy CEL compiler exposes the generator library to matchConditions, allowing a namespace-scoped policy to invoke generator.apply(namespace, resources) with an arbitrary target namespace. The validation in pkg/cel/policies/mpol/validate.go checks that the policy compiles but does not enforce namespace scope, and GenerateResources in pkg/cel/libs/context.go does not reject the cross-namespace target. A user who can create NamespacedMutatingPolicy objects in one namespace can cause the admission controller,	9.6	More Details

	operating with cluster-wide privileges, to create ConfigMaps, NetworkPolicies, Secrets, RoleBindings, and other resources in another namespace, enabling unauthorized modification and potential privilege escalation. This issue is fixed in version 1.18.2.		
CVE-2026-77016	The Workeera WordPress plugin before 1.0.6 does not restrict which values may be written to a user's own candidate profile, and does not validate or contain the stored file path before deleting it, allowing users with a role as low as subscriber to delete arbitrary files on the server.	9.6	More Details
CVE-2026-77532	A malicious actor with access to an adjacent network could exploit a Buffer Overflow vulnerability found in a DHCPv6-enabled EdgeMAX EdgeSwitch to initiate a Remote Code Execution on such device.	9.6	More Details
CVE-2026-59354	In versions of Spring Security's OAuth2 Authorization Server module 7.0.0 through 7.0.4, when Dynamic Client Registration is explicitly enabled, the registration endpoint performs insufficient validation of certain client metadata fields supplied by the registering client. An attacker who possesses a valid Initial Access Token can register a malicious client with crafted metadata, which, depending on server configuration and how the metadata is later rendered or used, may result in Stored Cross-Site Scripting (XSS), Privilege Escalation, or Server-Side Request Forgery (SSRF).	9.6	More Details
CVE-2026-80585	In the Linux kernel, the following vulnerability has been resolved: mptcp: fastopen: only mark MPTFO subflows with SYN data Passive TCP Fast Open accepts a valid-cookie SYN even when it carries no data. In that case the child socket's receive queue is intentionally left empty. mptcp_fastopen_subflow_synack_set_params() set is_mptfo before checking for queued SYN data. That made data-less TFO SYNs hit a WARN and, if the warning was non-fatal, left stale MPTFO state behind. The stale flag could later trigger a state-confusion bug in check_fully_established(). Only mark the subflow as MPTFO after confirming that an SKB was queued. Return quietly when the receive queue is empty. Note that mptcp_subflow_context's is_mptfo field is now not just about subflows where the TFO was present, but about MPTFO subflow that consumed SYN data. Only having a valid cookie but not carrying data is not really "doing TFO".	9.4	More Details
CVE-2026-59270	Spring Security's embedded UnboundID LDAP server (UnboundIdContainer) unconditionally registers an administrative credential and binds its listener to all available network interfaces. Spring Security 7.1.0 Spring Security 7.0.0 - 7.0.6 Spring Security 6.5.0 - 6.5.11 Spring Security 6.4.0 - 6.4.18 Spring Security 5.8.0 - 5.8.27 Spring Security 5.7.0 - 5.7.25	9.4	More Details
CVE-2026-74751	In the Linux kernel, the following vulnerability has been resolved: riscv: lib: Fix ZBB strnlen reading past count boundary The ZBB-optimized strnlen loop loads one word ahead before checking the aligned boundary: REG_L t1, SZREG(t0) // load next word addi t0, t0, SZREG // advance orc.b t1, t1 bgeu t0, t4, 4f // boundary check AFTER load where t4 = (s + count) & -SZREG. When s is aligned and count is a multiple of SZREG, t4 equals s + count and the loop loads a full word starting at exactly s + count. If s + count falls on a page boundary with the next page unmapped, this faults. Fix by computing the aligned boundary from the last valid byte (s + count - 1) instead of s + count. This makes the loop stop at the word containing the last valid byte rather than potentially loading the word after it. The count == 0 case is already handled by the beqz early exit. Also add a pre-loop guard (bgeu t0, t4) for the case where all valid bytes fit within the first word. With the adjusted boundary, t4 can equal t0, and entering the loop with stale register state from the first-word processing would produce incorrect results. The final minu clamp ensures the result is still correct when the last loaded word extends past s + count - 1 within the same aligned word.	9.4	More Details
CVE-2026-59111	Improper neutralization of special elements used in an OS command ('OS command injection') vulnerability in Digitální a informační agentura (DIA) eObčanka-Identifikace on MacOS enables an attacker to register a custom URL scheme (czeeopauth://) for parameterized application execution. Prior to version 3.6.0, incoming URL parameters were passed to the compiled AppleScript wrapper using concatenation without sufficient sanitization.	9.3	More Details
CVE-2026-80551	In the Linux kernel, the following vulnerability has been resolved: s390/vfio_ccw: Ensure first IDAW remains constant The first IDAW in a list does not need to be on a 2K/4K boundary like all others, and so is read separately to accurately calculate the size of the buffer needed to read the full IDAL. Verify that the address found in the first IDAW is unchanged between reads, to ensure a consistent set of IDAWs being worked with.	9.3	More Details
CVE-2026-51106	An issue in TokTok qTox v1.18.4 allows a local attacker to cause a denial of service via the src/persistence/serialize.cpp component	9.3	More Details
CVE-2026-81293	Unauthenticated SQL Injection in WP Data Access <= 5.5.81 versions.	9.3	More Details
CVE-2026-81756	Unauthenticated SQL Injection in Smart Marketing SMS and Newsletters Forms <= 5.1.24 versions.	9.3	More Details
CVE-2026-80554	In the Linux kernel, the following vulnerability has been resolved: s390/vfio_ccw: Limit the number of channel program segments The processing of channel programs, and the CCWs within them, is done recursively. As such, there is an arbitrary (but not architectural) limit to the number of CCWs that can exist in a single channel program. The vfio-ccw logic breaks these channel programs into segments whenever it encounters a Transfer-In-Channel (TIC) CCW, and the combined number of segments count towards the global limit. Impose an equivalent	9.3	More Details

	limit to the number of segments until such logic can be made non-recursive.		
CVE-2026-81763	Unauthenticated SQL Injection in Throws SPAM Away <= 3.8.2 versions.	9.3	More Details
CVE-2026-77012	The 爱采集数据采集和发布插件 WordPress plugin through 1.0.0 does not require a per-install secret for one of its unauthenticated endpoints, relying on a hardcoded default, and does not validate the URLs or destination paths it is given, allowing unauthenticated attackers to read arbitrary files from the server, force it to issue arbitrary requests and retrieve the responses, and write attacker-supplied content outside the uploads directory.	9.3	More Details
CVE-2026-80671	In the Linux kernel, the following vulnerability has been resolved: perf sched: Fix register_pid() overflow, strcpy, and BUG_ON register_pid() has several issues when processing untrusted perf.data: 1. Integer overflow: (pid + 1) * sizeof(struct task_desc *) can wrap to a small value on 32-bit systems when pid is large (e.g. 0x40000000), causing realloc to return a tiny buffer followed by out-of-bounds writes in the initialization loop. 2. Heap buffer overflow: strcpy(task->comm, comm) copies the untrusted comm string into a fixed 20-byte COMM_LEN buffer with no length check. 3. BUG_ON on allocation failure: perf.data is untrusted input, so allocation failures should be handled gracefully rather than killing the process. 4. Realloc of sched->tasks assigned directly back, leaking the old pointer on failure; nr_tasks incremented before the realloc, leaving corrupted state on failure. Cap pid at PID_MAX_LIMIT (4194304, matching the kernel's maximum on 64-bit), replace strcpy with strlcpy, guard against NULL comm, replace BUG_ON with NULL returns using safe realloc patterns, and add NULL checks in callers that dereference the result.	9.3	More Details
CVE-2026-78260	Unauthenticated SQL Injection in Epayco <= 8.4.6 versions.	9.3	More Details
CVE-2026-16279	An Improper Authorization vulnerability affecting 3DPassport in 3DSwymer from Release 3DEXPERIENCE R2023x through Release 3DEXPERIENCE R2026x could allow an attacker to gain access to some user accounts.	9.3	More Details
CVE-2026-80693	In the Linux kernel, the following vulnerability has been resolved: idpf: bound interrupt-vector register fill to the allocated array idpf_get_reg_intr_vecs() fills the caller-allocated reg_vals[] array from the VIRTCHNL2_OP_ALLOC_VECTORS reply in adapter->req_vec_chunks, bounding its inner loop only by the per-chunk num_vectors. The array is sized separately: idpf_intr_reg_init() allocates kzalloc_objs(struct idpf_vec_regs, total_vecs) from caps.num_allocated_vectors and only checks the returned count after the fill. The sum of per-chunk num_vectors is never reconciled against total_vecs, so a reply with a small num_allocated_vectors but chunks summing higher writes past the end of reg_vals[]. Impact: a control plane (a PF or hypervisor device model) that returns a VIRTCHNL2_OP_ALLOC_VECTORS reply whose per-chunk num_vectors sum exceeds num_allocated_vectors writes struct idpf_vec_regs entries past the end of the reg_vals kmalloc allocation (KASAN slab-out-of-bounds write). Bound the fill loop to the array capacity passed in by the callers, mirroring the sibling idpf_vport_get_q_reg(). The existing num_regs < num_vecs check then rejects an undersized reply without the out-of-bounds write happening first.	9.3	More Details
CVE-2026-80684	In the Linux kernel, the following vulnerability has been resolved: KVM: s390: pci: Fix NULL dereference on AIBV allocation failure The airq_iv_create() can return NULL on failure, but the return value was never checked. If it fails, zdev->aibv will be NULL and fail when dereferenced in kvm_zpci_set_airq(). Add a NULL check and free the previously allocated AISB bit and zdev->aisb on failure.	9.3	More Details
CVE-2026-32479	Unauthenticated SQL Injection in Visitor Traffic Real Time Statistics Pro <= 11.17 versions.	9.3	More Details
CVE-2026-78288	Unauthenticated SQL Injection in Beautiful Taxonomy Filters <= 2.4.6 versions.	9.3	More Details
CVE-2026-51713	Incorrect access control in the setManualDialCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to manipulate WAN dial state via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.1	More Details
CVE-2026-51711	Incorrect access control in the setWiFiWpsStart function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to open a wireless pairing window via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.1	More Details
CVE-2026-51710	Incorrect access control in the setParentalRules function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to alter parental-control behavior via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.1	More Details
CVE-2026-	Wazuh is an open-source security platform providing unified XDR and SIEM protection for endpoints and cloud workloads. In versions 4.4.0 through 4.14.6, a party holding the cluster key can write, overwrite, or delete arbitrary files under /var/ossec on worker nodes, leading to remote code execution as root. During cluster file synchronization, the non-merged branch of update_master_files_in_worker() moves each staged file to a destination derived only from safe_join(), which confines the path to /var/ossec but never verifies that the file lands in the directory declared by its cluster_item_key. Because the destination check present on the primary	9.1	More Details

61800	node and on the worker's merged branch was not applied, a peer can place files at attacker-chosen locations under /var/ossec, including paths that are executed as root, and the delete branch has the same gap. This is an incomplete fix for CVE-2026-30893, which addressed traversal outside /var/ossec but left this path able to redirect files anywhere within it. This issue is fixed in version 4.14.7.		
CVE-2026-77542	A malicious actor with access to the network and high privileges could exploit an Improper Input Validation vulnerability found in UID Enterprise Agent to execute a Command Injection on the host device.	9.1	More Details
CVE-2026-51701	Incorrect access control in the setMacFilterRules function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to change device access control via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.1	More Details
CVE-2026-51700	Incorrect access control in the setWiFiAdvancedCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to degrade wireless behavior via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.1	More Details
CVE-2026-51698	Incorrect access control in the setUrlFilterRules function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to alter browsing policies via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.1	More Details
CVE-2026-51152	Server-side request forgery (SSRF) in the /har/test endpoint in QD 20220208 through 20250803. Fetcher.build_request() in libs/fetcher.py constructs an httpclient.HTTPRequest from user-supplied JSON without validating URL scheme, host, or IP range. The /har/test handler does not require authentication, enabling unauthenticated remote attackers to force the QD server to send arbitrary HTTP requests to internal network resources and cloud metadata endpoints. validate_cert is set to False, disabling TLS verification.	9.1	More Details
CVE-2026-78274	Editor Arbitrary File Upload in Fluent Boards Pro <= 2.0.11 versions.	9.1	More Details
CVE-2026-51697	Incorrect access control in the setIptvCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to alter IPTV service configuration via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.1	More Details
CVE-2026-51717	Incorrect access control in the setOpModeCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to change the device operating mode via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.1	More Details
CVE-2026-77541	A malicious actor with access to the network and high privileges could exploit an Improper Access Control vulnerability found in UniFi Network Application to escalate privileges within the UniFi Network Application.	9.1	More Details
CVE-2026-16947	The Total processing card payments for WooCommerce WordPress plugin through 7.3 does not validate a user-supplied path before using it to build a server-side verification request, and does not verify the authenticity of the response, allowing unauthenticated attackers to redirect that request to an arbitrary host (disclosing the merchant's payment-gateway credentials) and to forge a success response that marks arbitrary WooCommerce orders as paid.	9.1	More Details
CVE-2026-51720	Incorrect access control in the delIpPortFilterRules function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to remove firewall filter rules via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.1	More Details
CVE-2026-81098	The Telnyx MCP server exposed its HTTP transport on every interface and did not require a caller credential. packages/mcp-server/src/http.ts served MCP on the root path with a listener bound to all interfaces and parsed the caller's authentication headers in a mode that did not fail when they were absent, so a request without any credential completed initialisation and dispatched tools. Dispatch forwarded the server's own stored credentials, the Telnyx API key and client secret together with the code-execution key, to the upstream endpoint, so an unauthenticated caller able to reach the port acted with them. The current code defaults the host to loopback, requires a server API key, and enforces it in middleware.	9.1	More Details
CVE-2026-81094	The mcp-router CLI served its MCP aggregator on every interface and enforced authentication only when the operator asked for it. The serve command in apps/cli/src/commands/serve.ts defaulted its host to the all-interfaces address on a fixed port, and required a token only when the corresponding flag was supplied, so a default invocation exposed the aggregator, and every MCP server it fronted, to anyone able to reach the port. Release 0.6.3 defaults the host to the loopback address and refuses to start without a token whenever the host it is given is not a loopback address; no earlier release carries either check.	9.1	More Details
CVE-2026-59283	Applications that evaluate Spring Expression Language (SpEL) expressions using SimpleEvaluationContext may be vulnerable to a safety guard bypass when the SpEL expression compiler is active. Spring Framework 7.0.0 - 7.0.8 Spring Framework 6.2.0 - 6.2.19 Spring Framework 6.1.0 - 6.1.28 Spring Framework 6.0.0 - 6.0.30 Spring Framework 5.3.0 - 5.3.49 Spring Framework 5.2.25.RELEASE and earlier	9.1	More Details
CVE-			More

2026-59682	Arbitrary file overwrite via SAVE_PROFILE message in OpenRGB. This issue affects OpenRGB through 1.0rc3.	9.1	Details
CVE-2026-57499	Liman is open source server management software. Prior to 2.2.2 - 1103, an OS command injection vulnerability in the log rotation configuration endpoint allows an authenticated administrator to execute arbitrary operating system commands on the Liman server. The `ip_address` parameter is embedded directly into a shell command without sanitization, enabling shell escape via single-quote injection. This is fixed in 2.2.2 - 1103.	9.1	More Details
CVE-2026-51736	Incorrect access control in the clearSyslog function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to erase system logs via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.1	More Details
CVE-2026-77535	A malicious actor with access to the network and high privileges could exploit an Improper Input Validation vulnerability found in UniFi Network Application to execute a Command Injection on an adopted device.	9.1	More Details
CVE-2026-51731	Incorrect access control in the delVlanCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to remove VLAN entries via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.1	More Details
CVE-2026-50152	Ceph is an open-source distributed storage platform providing object, block, and file storage. In versions prior to 20.2.4 and 19.2.6, the Monitor subscription handler fails to properly authorize access to the configuration-key store, allowing any CephX user with only `mon allow r` capabilities to read the entire store by sending a single crafted MMonSubscribe message. The config-key store holds sensitive secrets including OSD LUKS disk-encryption passphrases and, on cephadm-managed clusters, the SSH private key that cephadm uses to reach every host in the cluster. Because that key grants root on every node under the default cephadm configuration, a low-privileged read-only account can escalate to full cluster and host compromise. This issue is fixed in versions 20.2.4 and 19.2.6	9.1	More Details
CVE-2026-77539	A malicious actor with access to the network and high privileges could exploit an Improper Input Validation vulnerability found in UniFi OS Server to execute a Command Injection on the host device.	9.1	More Details
CVE-2026-51730	Incorrect access control in the delWiFiAclRules function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to remove Wi-Fi ACL rules via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.1	More Details
CVE-2026-51729	Incorrect access control in the delDevice function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to request deletion of a managed slave device via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.1	More Details
CVE-2026-51726	Incorrect access control in the delParentalRules function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to remove parental-control rules via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.1	More Details
CVE-2026-51725	Incorrect access control in the NTPSyncWithHost function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to change the device clock via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.1	More Details
CVE-2026-77540	A malicious actor with access to the network and high privileges could exploit an Improper Input Validation vulnerability found in UniFi OS Server to execute a Command Injection on the host device.	9.1	More Details
CVE-2026-51722	Incorrect access control in the setWiFiRepeaterCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to repoint the device to an attacker-controlled upstream Wi-Fi via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.1	More Details
CVE-2026-51721	Incorrect access control in the setPairCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to alter the mesh pairing state via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.1	More Details
CVE-2026-51681	Incorrect access control in the setRemoteCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to expose WAN-side administration via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.1	More Details
CVE-2026-51680	Incorrect access control in the setLedCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to modify LED behavior via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.1	More Details
CVE-2026-51679	Incorrect access control in the setPasswordCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to change the administrator account via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.1	More Details
CVE-2026-	Incorrect access control in the setUPnPCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to change UPnP service state via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.1	More Details

51677			
CVE-2026-51622	Incorrect access control in the getWanCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain WAN configuration data via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.1	More Details
CVE-2026-51626	Incorrect access control in the getWiFiWpsCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain WPS configuration, including the current PIN, via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.1	More Details
CVE-2026-51628	Incorrect access control in the getGenerateWiFiWpsPin function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to generate and retrieve a new WPS PIN via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.1	More Details
CVE-2026-51636	Incorrect access control in the getWiFiAclRules function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain Wi-Fi ACL rules via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.1	More Details
CVE-2026-51643	Incorrect access control in the getNtpCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain NTP configuration and current time data via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.1	More Details
CVE-2026-51646	Incorrect access control in the getParentalRules function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain parental-control rules via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.1	More Details
CVE-2026-51649	Incorrect access control in the getDiagnosisCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain diagnostic configuration and ping log contents via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.1	More Details
CVE-2026-51657	Incorrect access control in the getSyslogCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain syslog-related configuration via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.1	More Details
CVE-2026-51660	Incorrect access control in the getIpPortFilterRules function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain IP and port filtering rules via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.1	More Details
CVE-2026-55247	plone.app.event provides the event content type for Plone. Prior to versions 5.2.4 and 6.0.1, the iCalendar import in src/plone/app/event/ical/importer.py accepts insufficiently restricted calendar and event URLs, does not adequately bound downloaded bytes or imported events, and commits work per event. A logged-in editor can make the server request internal network resources or local calendar files, exhaust resources and take the site offline, and store a malicious event URL that executes script in another user's browser. The fix restricts accepted URLs, applies MAXIMUM_ICAL_IMPORT_SIZE_BYTES and MAXIMUM_ICAL_IMPORT_EVENTS limits, uses transaction savepoints, and validates event URLs. This issue is fixed in versions 5.2.4 and 6.0.1.	9.1	More Details
CVE-2026-82539	A vulnerability was determined in TOTOLINK A720R 4.1.5cu.630_B20250509. This impacts the function setMacFilterRules of the file cstecgi.cgi of the component MAC Filtering. Executing a manipulation of the argument desc can lead to memory corruption. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.	9.1	More Details
CVE-2026-55248	plone.app.portlets provides portlets and a Plone-specific user interface for plone.portlets. Prior to 5.0.8, 6.0.4, and 7.0.2, a member who can add an RSS portlet can set its feed URL to a very large response, causing src/plone/app/portlets/portlets/rss.py to download and retain excessive data in memory and deny service. The same RSS URL handling accepts internal hosts, IP addresses, single-word domains, and explicit ports, allowing server-side requests that can probe internal network services and open ports. A malicious feed item can also supply a JavaScript URL that is retained as the item link and can execute script when used by a victim. The affected logic includes _rss_feed_url_validator, _normal_url_validator, RSSFeed._retrieveFeed, RSSFeed._buildItemDict, and the FEED_DATA in-memory cache. This issue is fixed in versions 5.0.8, 6.0.4, and 7.0.2.	9.1	More Details
CVE-2026-55511	Yamcs is a mission control framework. Prior to 5.12.8 and 5.13.2, Yamcs allows a user with SystemPrivilege.ControlArchiving to create a double-quoted StreamSQL column name that is interpolated into generated Java source by Expression.fillCode_InputDefVars and Expression.sanitizeName. A sum aggregate reaches yamcs-core/src/main/java/org/yamcs/yarch/streamsql/CompilableAggregateExpression.java and yamcs-core/src/main/java/org/yamcs/yarch/streamsql/funct/SumExpression.java through SelectExpression.compile, where Janino SimpleCompiler.cook compiles the injected source. POST /api/archive/{instance}:executeSql can therefore execute arbitrary Java in the Yamcs server process, exposing mission data and credentials and permitting telemetry tampering or denial of service. This issue is fixed in versions 5.12.8 and 5.13.2.	9.1	More Details
CVE-2025-51679	An issue was discovered in openRISC OR1200 commit 83ac6b. A mismatch between the RTL and netlist can lead to unexpected behavior.	9.1	More Details
CVE-	IBM Concert 1.0.0 through 2.3.1 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL		More

2026-3627	statements, which could allow the attacker to view, add, modify, or delete information in the back-end database.	9.1	Details
CVE-2026-51661	Incorrect access control in the getPortForwardRules function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain port-forwarding rules via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.1	More Details
CVE-2026-70419	Dell Cloud Disaster Recovery, versions 20.2 and prior, 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.	9.1	More Details
CVE-2026-82078	An unsafe dynamic class loading vulnerability exists in the database connection utilities of PaperCut MF and PaperCut NG. The application instantiates database driver classes based on configurable driver names without validating against an allowlist of approved drivers. If an attacker can manipulate system configuration parameters, this enables the execution of arbitrary Java bytecode residing on the application classpath under the security context of the PaperCut server process.	9.1	More Details
CVE-2026-82244	Budibase versions before 3.41.3 contain a remote code execution vulnerability in plugin handling that allows authenticated admin users to execute arbitrary code by uploading a malicious plugin tarball. The server calls eval() on plugin JavaScript files without sandboxing in the main Node.js process, enabling attackers to exfiltrate environment variables and credentials with root privileges in default deployments.	9.1	More Details
CVE-2026-75332	Zyplayer-Doc <=1.0.0 is vulnerable to Server-Side Request Forgery (SSRF) via WikiPageWebService.download().	9.1	More Details
CVE-2026-80670	In the Linux kernel, the following vulnerability has been resolved: perf tools: Use perf_env__get_cpu_topology() in machine__resolve() machine__resolve() accesses env->cpu[al->cpu].socket_id after checking al->cpu >= 0 and env->cpu != NULL, but without validating al->cpu against env->nr_cpus_avail. Since al->cpu comes from the untrusted perf.data sample, a crafted file with a large CPU index causes an out-of-bounds heap read. Use perf_env__get_cpu_topology() which validates both NULL and bounds. Also bounds-check al->cpu before the cast to struct perf_cpu (int16_t): without this, values like 65536 silently truncate to 0, bypassing the accessor's internal check and returning CPU 0's topology.	9.1	More Details
CVE-2026-51676	Incorrect access control in the setAccessDeviceCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to alter access-device policies via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.1	More Details
CVE-2026-51675	Incorrect access control in the setWanIeCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to reconfigure uplink settings via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.1	More Details
CVE-2026-80603	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_conntrack_irc: fix parse_dcc() off-by-one OOB read parse_dcc() treats data_end as an inclusive end pointer, but its only caller passes data_limit = ib_ptr + datalen, which points one past the last valid byte. The newline search loop iterates while tmp <= data_end, so when no newline is present, *tmp is read at tmp == data_end, one byte beyond the region filled by skb_header_pointer(). irc_buffer is kmalloc'd as MAX_SEARCH_SIZE + 1 bytes and datalen is capped at MAX_SEARCH_SIZE, so the stray read does not fault. The byte is uninitialized or stale; if it contains an ASCII digit, simple_strtoul will consume it and produce a wrong DCC IP or port in the conntrack expectation. The extra allocation byte is also a fragile guard: if the cap or allocation size changes, this becomes a real out-of-bounds read. Change the loop and its post-loop check to use strict less-than, consistent with the caller's exclusive-end convention. Update the function comment accordingly.	9.1	More Details
CVE-2026-51672	Incorrect access control in the getRoamingCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain the roaming enablement flag via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.1	More Details
CVE-2026-75896	Use of Hard-coded Credentials vulnerability in TÜBİTAK BİLGEM Software Technologies Research Institute Liderahenk allows Try Common or Default Usernames and Passwords. This issue affects Liderahenk: before 3.5.5.	9.1	More Details
CVE-2026-51669	Incorrect access control in the getPairCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain pairing and mesh-slave configuration via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	9.1	More Details
CVE-2026-75340	The device metadata import interface /device/instance/{productId}/property-metadata/import of jetlinks community 2.11 is vulnerable to Server-side request forgery (SSRF).	9.1	More Details
CVE-2026-82691	A vulnerability has been found in D-Link DNS-320L, DNS-327L, DNS-340L and DNS-345 up to 20260717. Affected by this issue is some unknown functionality of the file /cgi-bin/usb_device.cgi of the component CGI Handler. Such manipulation of the argument f_ups_ip leads to os command injection. The attack may be performed from remote. The exploit has been disclosed to the public and may be used.	9.1	More Details
	A flaw has been found in D-Link DNS-327L and DNS-340L up to 20260717. Affected by this vulnerability is an		

CVE-2026-82690	unknown functionality of the file /cgi-bin/ve_mgr.cgi. This manipulation of the argument f_dev causes os command injection. The attack is possible to be carried out remotely. The exploit has been published and may be used.	9.1	More Details
CVE-2026-82688	A security vulnerability has been detected in D-Link DNS-340L and DNS-345 1.01B04/1.03B06/1.04.B02/1.05b04. This impacts an unknown function of the file /cgi-bin/virtual_vol.cgi of the component Virtual Volume Handler. The manipulation of the argument f_sharename/f_target/f_name leads to os command injection. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	9.1	More Details
CVE-2026-42007	An attacker that has valid credentials can use a Sieve script with the editheader extension to trigger a use-after-free in the mail editing code, and to write memory contents beyond the intended buffer into the delivered mail. This causes memory leak and opportunity to do memory corruption during mail delivery, which can crash the delivery process and may allow execution of arbitrary code in the context of that process. Disable the Sieve editheader extension. Update to non-vulnerable version. No publicly available exploits are known.	9.1	More Details
CVE-2026-82872	ToolJet before v3.16.208 fails to validate that the path organizationId matches the authenticated user's workspace before performing ToolJet DB table operations. A workspace admin can create, view, and delete database tables in another workspace by replacing the organizationId parameter in table-management API requests.	9.1	More Details
CVE-2026-82454	The Omnivore API (packages/api) before the fix in commit abf53d6 contains an authentication bypass in Apple sign-in token verification. The decodeAppleToken function extracted the 'alg' field from the attacker-supplied JWT header and passed it as the sole allowed algorithm to jwt.verify(). Using jsonwebtoken v8 (which does not validate key/algorithm compatibility), an attacker can set alg=HS256 and sign a forged token using Apple's publicly available RSA public key as the HMAC secret, bypassing signature verification and impersonating any Apple-linked account.	9.1	More Details
CVE-2026-77545	A malicious actor with access to the network, low privileges and under certain conditions could exploit an Active Debug Code vulnerability found in certain devices running UniFi OS to escalate privileges within such UniFi OS devices or instances.	9.0	More Details
CVE-2026-77549	A malicious actor with access to the network and under certain conditions could exploit an Improper Neutralization of CRLF Sequences vulnerability found in certain devices running UniFi OS to bypass authentication to such UniFi OS devices or instances.	9.0	More Details
CVE-2026-77551	A malicious actor with access to the network and under certain conditions could exploit an Improper Access Control vulnerability found in UniFi Connect Display Cast Pro to escalate privileges on the device.	9.0	More Details
CVE-2026-40541	An improper neutralization of input during web page generation ('Cross-site Scripting') vulnerability in extract domain in Synology Chat Server before 2.4.5-22148 allows remote authenticated users, via a UI interaction, to read or write arbitrary files and conduct denial-of-service attacks in DSM.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2026-82653	SiYuan before v3.8.1 contains a stored cross-site scripting vulnerability in confirmDialog() where unescaped package names and notebook names are interpolated directly into innerHTML assignments. Attackers can submit malicious bazaar packages with HTML/script payloads in the name field that execute in users' browsers when uninstalling packages or unlocking encrypted notebooks.	8.9	More Details
CVE-2026-82654	SiYuan before v3.8.1 fails to properly escape block name, alias, and memo fields in hint, backlink, and breadcrumb rendering functions. Attackers can set a block's name to contain HTML/script tags that execute when another user views documents referencing or displaying that block.	8.9	More Details
CVE-2025-30156	Ceph is an open-source distributed storage platform providing object, block, and file storage. In versions prior to 20.2.4 and 19.2.6, the CephX authentication protocol encrypts tickets with AES-128-CBC in an unauthenticated mode that uses a hard-coded initialization vector and no message authentication, allowing an attacker to forge credentials and gain cluster-wide access. Because the ciphertext is malleable and the monitor will encrypt attacker-chosen entity names, an attacker holding one low-privilege key and able to observe CephX traffic can use the monitor as an encryption oracle and splice ciphertext blocks into valid tickets for privileged entities such as Manager, MDS, and OSD. The same lack of authentication also lets an attacker with CephX permissions escalate privileges by flipping a single bit in a service ticket to set its allow_all field to true. This issue is fixed in versions 20.2.4 and 19.2.6.	8.9	More Details
CVE-2026-63041	Reliance on Untrusted Inputs in a Security Decision vulnerability in Apache APISIX. This vulnerability allows an attacker to escalate privilege or perform an authorization bypass by sending certain values that the attach-consumer-label plugin does not sanitise correctly. This issue affects Apache APISIX: from 3.11.0 through 3.17.0. Users are recommended to upgrade to version 3.18.0, which fixes the issue.	8.8	More Details
	Pake before 3.13.1 joins the JavaScript-supplied filename for the download_file Tauri command onto the		

CVE-2026-82635	user's Downloads directory with no sanitization. A filename containing path traversal sequences (for example ../Library/LaunchAgents/com.evil.plist) or an absolute path resolves outside ~/Downloads. The command then fetches attacker-controlled content from the supplied URL (via Rust HTTP, not the browser) and writes it to that path. A script that can invoke the command can overwrite user-writable files and install persistence (macOS LaunchAgents, Linux autostart, Windows Startup), leading to code execution in the user account. All desktop apps generated from an affected Pake tree expose the same command.	8.8	More Details
CVE-2026-82642	Readest is an open-source e-book reader built on Tauri. In versions prior to 0.11.16, EPUB chapter HTML is sanitized with DOMPurify using a configuration that forbade only the <script> tag (FORBID_TAGS: ['script']) in apps/readest-app/src/services/transformers/sanitizer.ts. DOMPurify does not parse the contents of the srcdoc attribute on <iframe> elements, treating it as an opaque string attribute, so an attacker who can get an <iframe> element to survive sanitization can embed a complete HTML document containing a <script> tag inside srcdoc and have it execute when the browser renders the iframe. The content iframe is configured with sandbox="allow-same-origin allow-scripts", so script executing inside it shares the parent origin and can reach parent.parent.__TAURI_INTERNALS__.invoke(...), giving access to every Tauri IPC command the application is permitted to use, which escalates to arbitrary code execution. The payload can be made invisible (zero-size, transparent iframe) so the reader sees only normal book text. Version 0.11.16 hardened the sanitizer configuration by adding 'iframe', 'object' and 'embed' to FORBID_TAGS and adding 'srcdoc' to FORBID_ATTR.	8.8	More Details
CVE-2026-18965	PayRange API is missing proper authorization on management endpoints, which allows verbose details of every device on the PayRange network to be publicly accessible, with or without an account.	8.8	More Details
CVE-2026-74770	Dell PowerProtect One, versions 20.1.0.0 and below, 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 Code execution.	8.8	More Details
CVE-2026-82217	In Eclipse Theia versions 1.73.0 up to but not including 1.75.0, the AI "Agent Mode" file-change tools (writeFileContent, suggestFileContent, and the replacement and state helpers) resolved a model-supplied file path without a workspace-containment check. A crafted relative path such as ../.bashrc, an absolute path, or a ~-expanded path could therefore write or delete files outside the workspace with the privileges of the Theia backend OS user. Because the path argument is influenced by model output, it can be steered through indirect prompt injection, and in Agent Mode writes are applied without a confirmation dialog. Writing to a host-executed file such as a shell startup file or ~/.ssh/authorized_keys can escalate to code execution on the backend.	8.8	More Details
CVE-2026-80633	In the Linux kernel, the following vulnerability has been resolved: iommufd: Take dma_resv lock before dma_buf_unpin() in release path dma_buf_unpin() requires the caller to hold the exporter's dma_resv lock: void dma_buf_unpin(struct dma_buf_attachment *attach) { ... dma_resv_assert_held(dmabuf->resv); ... } iopt_release_pages() calls dma_buf_unpin() without taking that lock, so every iommufd_ioas_destroy()/iommufd_ioas_unmap() that releases the last reference on a DMABUF-backed iopt_pages triggers a WARN. This was hit while running tools/testing/selftests/iommu/iommufd: WARNING: drivers/dma-buf/dma-buf.c:1137 at dma_buf_unpin+0x62/0x70 RIP: 0010:dma_buf_unpin+0x62/0x70 Call Trace: <TASK> dma_buf_unpin+0x62/0x70 iopt_release_pages+0xe4/0x190 iopt_unmap_iova_range+0x1c7/0x290 iopt_unmap_all+0x1a/0x30 iommufd_ioas_destroy+0x1d/0x50 iommufd_fops_release+0x93/0x150 __fput+0xfc/0x2c0 __x64_sys_close+0x3d/0x80 do_syscall_64+0x65/0x180 </TASK> Take the dma_resv lock around dma_buf_unpin() in iopt_release_pages(), matching the iopt_map_dmabuf() convention. dma_buf_detach() acquires the reservation lock internally, so it must remain outside the locked region.	8.8	More Details
CVE-2026-81660	The Groundhogg — CRM, Newsletters, and Marketing Automation WordPress plugin before 4.5.13 does not validate or escape values submitted to some optional web form fields before storing them and outputting them back in an administrative area, allowing unauthenticated users to perform Stored Cross-Site Scripting attacks against high privilege users.	8.8	More Details
CVE-2026-12894	A flaw was found in the Qute template engine, which is used by Quarkus to generate dynamic content like HTML pages or emails. The issue exists in the component responsible for looking up data values (ReflectionValueResolver), which fails to properly block access to sensitive Java internal functions when processing certain data types like Enums. An attacker who can provide or influence the template text can exploit this bypass to take control of the server by executing unauthorized commands.	8.8	More Details
CVE-2026-81849	Improper limitation of a pathname to a restricted directory in the aws:downloadContent plugin in amazon-ssm-agent before 3.3.4515.0 might allow an authenticated remote user whose ssm:SendCommand permission is restricted to the AWS-DownloadContent document, to write arbitrary files outside the intended download directory with root privileges, via crafted object keys in the S3 source the document is directed to retrieve. This issue may lead to arbitrary code execution as root if specific sensitive files are overwritten. To remediate this issue, customers should upgrade amazon-ssm-agent to version 3.3.4515.0 or later.	8.8	More Details
CVE-2026-58474	whichllm before 0.5.16 contains a code injection vulnerability in the run and snippet commands that allows a remote attacker who controls a HuggingFace repository to achieve arbitrary code execution by crafting a malicious GGUF filename containing double quotes or other special characters. The script generation function in cli.py interpolates HuggingFace-derived values, including GGUF variant filenames from the Hub API siblings rfilename field, directly into Python source code without escaping, allowing the crafted filename to break out of the generated string literal and execute injected code on the user's machine before any	8.8	More Details

	model download occurs.		
CVE-2026-76585	The Customer Reviews for WooCommerce WordPress plugin before 5.118.0 does not sanitise and escape the content of customer reviews received via one of its endpoints, which could allow unauthenticated users to perform Stored Cross-Site Scripting attacks.	8.8	More Details
CVE-2026-58096	LcpDecodeConfig() did not validate the length of received endpoint discriminator options against the minimum required by RFC 1717. Undersized options would trigger an out-of-bounds write. A malicious PPP peer can exploit CVE-2026-58095 and CVE-2026-58096 to crash ppp(8) or potentially execute arbitrary code as root.	8.8	More Details
CVE-2026-82628	A vulnerability was found in Colorful iGameCenter 2.0.0.81. This vulnerability affects the function sub_11504 in the library WinRing0x64.sys of the component IOCTL Dispatch. Performing a manipulation of the argument PhysicalAddress/AlignNumer/AlignSize results in improper privilege management. Attacking locally is a requirement.	8.8	More Details
CVE-2026-80635	In the Linux kernel, the following vulnerability has been resolved: wifi: wcn36xx: fix OOB read from short trigger BA firmware response The firmware response length is only checked against sizeof(*rsp) (20 bytes), but when candidate_cnt >= 1, a 22-byte candidate struct is read at buf + 20 without verifying the response contains it. This causes an out-of-bounds read of stale heap data, corrupting the BA session state. Add validation that the response includes the candidate data.	8.8	More Details
CVE-2026-81271	Unauthenticated Cross Site Request Forgery (CSRF) in GeoDirectory <= 2.8.176 versions.	8.8	More Details
CVE-2026-39944	Ceph is an open-source distributed storage platform providing object, block, and file storage. In versions prior to 20.2.4 and 19.2.6, the RADOS Gateway (RGW) protects STS session tokens with an AES-128-CBC handler that provides no message authentication, allowing an attacker who holds any valid STS token to tamper with it undetected and escalate to full RGW administrative access. Because the ciphertext is unauthenticated, the attacker can perform a CBC bit-flip on the acct_type, perm_type, and is_admin fields of their own token, and a forged is_admin value triggers a global administrative override that bypasses all capability checks. The attack is reachable remotely over the RGW S3 endpoint and is a self-contained modification of a token the attacker already possesses, requiring no encryption oracle and no network observation. It requires only a single valid STS token, which need not carry any elevated privileges, with STS enabled. This issue is fixed in versions 20.2.4 and 19.2.6.	8.8	More Details
CVE-2026-5956	Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in Ankara Hosting Site Management Panel allows SQL Injection. This issue affects Site Management Panel: through 15062026.	8.8	More Details
CVE-2026-82278	BISHENG before 2.6.0 contains a remote code execution vulnerability in the workflow run_once endpoint that allows authenticated users to execute arbitrary Python code. Attackers can submit crafted Code node definitions to the POST /api/v1/workflow/run_once endpoint, which executes them with exec() without sandboxing, gaining access to filesystem, credentials, and internal network resources.	8.8	More Details
CVE-2026-68861	Dell PowerProtect One, versions 20.1.0.0 and below, 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 Remote execution.	8.8	More Details
CVE-2026-80237	EFence developed by Thinking Software Technology has an Arbitrary File Upload vulnerability. Authenticated remote attackers can upload and execute web shell backdoors, thereby enabling arbitrary code execution on the server.	8.8	More Details
CVE-2026-80348	TarsWeb enforces its per-application roles by calling AuthService from individual controller methods, and four methods in app/controller/patch/PatchController.js make no such call. uploadAndPublish accepts a package upload and then builds and dispatches a deployment task to every server matching the supplied application and module name, while its sibling uploadPatchPackage, which only stores the package, does check developer authorization first. The only precondition uploadAndPublish enforces is that the named server is registered, and any registered server in the installation satisfies it. downloadPackage and deletePatchPackage select a package by an unscoped sequential primary key covering every application's uploads, and setPatchPackageDefault changes which package a given application deploys by default. Any authenticated account, including one holding a role scoped to a single unrelated application, can therefore push a package to and trigger its deployment on any server the console manages, retrieve or delete any other application's package, and change which package is deployed by default.	8.8	More Details
CVE-2026-80608	In the Linux kernel, the following vulnerability has been resolved: accel/amdxdna: Fix iommu domain lifetime race during device removal When force_iova mode is enabled, amdxdna_remove() frees xdna->domain. If amdxdna_gem_obj_free() is called after device removal, it may attempt to access xdna->domain, resulting in a use-after-free. Fix the race by adding freeing xdna->domain as a managed release action, so its lifetime is managed by DRM and remains valid until all managed resources are released.	8.8	More Details
CVE-2026-80692	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_sync: hold conn in hci_connect_acl/le_sync() callbacks There is theoretical UAF if the conn is freed while the hci_sync task is running. Hold refcount to avoid that.	8.8	More Details

CVE-2026-80604	In the Linux kernel, the following vulnerability has been resolved: HID: core: Fix OOB read in hid_get_report for numbered reports When a caller passes a size of 0 to hid_report_raw_event() for a numbered report, the function originally called hid_get_report() before performing any size validation. Inside hid_get_report(), if the report is numbered (report_enum->numbered is true), it unconditionally dereferences data[0] to extract the report ID. With a size of 0, this results in an out-of-bounds read or kernel panic. Fix this by moving the numbered report size validation check before the call to hid_get_report(), ensuring that size is at least 1 before dereferencing the data pointer.	8.8	More Details
CVE-2026-19042	A command injection vulnerability in TeamViewer Full Client and Host for Linux prior to version 15.81.5 allows a remote attacker to execute arbitrary commands in the context of the current user via a specially crafted URL sent through the out-of-session chat feature. Exploitation requires user interaction by clicking the malicious link.	8.8	More Details
CVE-2026-80601	In the Linux kernel, the following vulnerability has been resolved: batman-adv: gw: acquire ethernet header only after skb realloc The pskb_may_pull() called by batadv_get_vid() could reallocate the buffer behind the skb. Variables which were pointing to the old buffer need to be reassigned to avoid an use-after-free.	8.8	More Details
CVE-2026-77018	The Workeera WordPress plugin before 1.0.6 does not restrict which profile values a candidate may submit, nor validate the type of the file it subsequently writes into a publicly reachable directory, allowing users with a role as low as subscriber to upload arbitrary files and achieve remote code execution.	8.8	More Details
CVE-2026-10036	SpeechBrain before 1.1.1 contains an arbitrary code execution vulnerability that allows attackers to execute arbitrary code by supplying a crafted CKPT.yaml checkpoint metadata file parsed with PyYAML's unsafe loader during candidate enumeration in Checkpointer.recover_if_possible(). Attackers can embed malicious Python object construction tags such as !!python/object/apply in any CKPT.yaml file within the configured checkpoint path to trigger code execution during candidate discovery, even if the malicious checkpoint is never selected for recovery.	8.8	More Details
CVE-2026-80638	In the Linux kernel, the following vulnerability has been resolved: ocfs2: fix out-of-bounds write in ocfs2_remove_refcount_extent [BUG] Unlinking a refcounted file whose refcount tree has leaf blocks triggers a fortify panic due to an out-of-bounds write. [CAUSE] When the last leaf block is removed from a refcount tree, ocfs2_remove_refcount_extent() converts the root back to leaf mode with a bulk memset on &rb->rf_records. rf_records sits in an anonymous union with rf_list. rf_list.l_tree_depth aliases rf_records.rl_count, and is 0 for a single-level tree. With rl_count equal to 0, the memset writes past the 16-byte declared size of rf_records, which the fortify checker catches. [FIX] Replace the bulk memset on &rb->rf_records with a correctly-bounded memset on rl_recs[] alone, after setting rl_count to the correct value.	8.8	More Details
CVE-2026-54721	Silverstripe UserForms provides a visual form builder for the Silverstripe CMS. From 6.0.0 until 6.4.9, 7.0.7, and 7.1.1, the userform email recipient subject field in the CMS accepts a specially crafted payload that can be interpreted as executable server-side code. An authenticated CMS user with permission to configure a UserForms email recipient can use the subject field to run arbitrary code on the server, compromising confidentiality, integrity, and availability. This issue is fixed in versions 6.4.9, 7.0.7, and 7.1.1.	8.8	More Details
CVE-2026-78333	The 12 Step Meeting List WordPress plugin before 3.19.17 does not sanitise and escape a value submitted by unauthenticated users before storing it in its activity log and outputting it back in an admin area page, leading to a Stored Cross-Site Scripting issue which could be used against high privilege users such as admin.	8.8	More Details
CVE-2026-18729	IBM Langflow OSS 1.0.0 through 1.11.1 could allow a remote authenticated attacker to execute arbitrary code due to improper control of generation of code.	8.8	More Details
CVE-2026-76639	Unitree G1 EDU firmware through 1.5.2 contains an unauthenticated remote code execution vulnerability that allows network-adjacent attackers to execute arbitrary commands as root by chaining three weaknesses: an unauthenticated WebRTC-to-DDS bridge on TCP port 9991, a static AES-128 key stored with world-readable permissions, and a path traversal flaw in the chat_go knowledge upload API. Attackers can publish DDS control messages to restart the bashrunner service, plant a malicious payload in its script execution directory via path traversal, and trigger execution of that payload as uid 0 through the bashrunner shell subprocess.	8.8	More Details
CVE-2026-82680	A weakness has been identified in D-Link DSM-G600 1.01. This affects an unknown function of the file /load_file.cgi of the component Multipart Handler. Executing a manipulation can lead to out-of-bounds write. The attack may be launched remotely. The exploit has been made available to the public and could be used for attacks.	8.8	More Details
CVE-2026-78236	An insecure PIN derivation mechanism in ABR allows a low-privileged user to escalate privileges to administrator by communicating over Cross-Process Communication (XPC) while masquerading as an Apple-signed process.	8.8	More Details
CVE-2026-75977	The Mang Board WP plugin for WordPress is vulnerable to Missing Authorization via Authentication Cookie Forgery in all versions up to, and including, 2.3.7. This is due to flawed HMAC generation in the mbw_get_hash_key() function that uses the current user's identity instead of the cookie username parameter when a WordPress user is logged in, combined with insufficient validation in mbw_validate_auth_cookie(). This makes it possible for authenticated attackers, with subscriber-level access and above, to forge administrator authentication cookies and change administrator passwords to achieve	8.8	More Details

	complete site takeover.		
CVE-2026-82072	Out of bounds read in V8 in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2026-58095	mp_Enddisc() used incorrect length calculations when formatting endpoint discriminator addresses for display, allowing a received endpoint option to overflow a global result buffer. A malicious PPP peer can crash ppp(8) or potentially execute arbitrary code as root.	8.8	More Details
CVE-2026-78037	Xiiaozet LK100W is vulnerable to OS command injection through its web-based management interface. An authenticated attacker may be able to execute arbitrary operating system commands with elevated privileges, potentially resulting in unauthorized access to sensitive information or complete device compromise.	8.8	More Details
CVE-2026-80202	Kimai before 2.56.0 does not enforce team-membership checks in TimesheetVoter::voteOnAttribute(), which maps permissions only to own_timesheet or other_timesheet. As a result, any authenticated user with ROLE_TEAMLEAD (or a role holding edit_other_timesheet/delete_other_timesheet) can read, modify, and permanently delete timesheets belonging to any user system-wide via the API, regardless of team membership. Timesheet IDs are sequential integers and trivially enumerable. ROLE_USER accounts are correctly restricted. (Note: the maintainers characterize this behavior as matching the documented permission model.)	8.8	More Details
CVE-2026-77966	The affected Ebyte product does not provide separation between limited and administrative management functions. A low privileged authenticated attacker could access security sensitive configuration functions and modify settings that affect the confidentiality, integrity, or availability of the device.	8.8	More Details
CVE-2026-80722	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: validate individual TWT params before driver setup ieee80211_process_rx_twt_action() only partially validates a received S1G TWT setup frame before queueing it. An individual agreement can therefore reach ieee80211_s1g_rx_twt_setup() with twt->length too short for the full struct ieee80211_twt_params. The individual path passes twt to drv_add_twt_setup(). Both the tracepoint and the driver callback consume the complete parameters block, not merely req_type. Do not pass a short individual agreement to the driver. Broadcast agreements remain unchanged because they are rejected locally after accessing only req_type. [edit commit message to not overclaim lack of validation nor understate driver impact]	8.8	More Details
CVE-2020-15874	An issue was discovered in LibreNMS 1.65. A remote authenticated attacker with normal privileges can execute arbitrary shell commands through a command injection in the /graph.php API endpoint.	8.8	More Details
CVE-2026-76060	An authenticated OS command injection vulnerability exists in ZoneMinder's event export functionality. The exportFile HTTP request parameter is passed unsanitized into a shell command executed via PHP's exec(), allowing any authenticated user with View Events permission to execute arbitrary operating system commands on the server.	8.8	More Details
CVE-2026-78257	Contributor PHP Object Injection in Booking and Rental Manager <= 2.7.5 versions.	8.8	More Details
CVE-2026-75814	The Ebyte device does not adequately verify the origin or authenticity of requests submitted to the web management interface. An unauthenticated remote attacker could persuade an authenticated administrator to visit a crafted page, causing unauthorized configuration changes or a disruption of device availability.	8.8	More Details
CVE-2026-80193	Kimai before 2.62.0 fails to validate create_other_timesheet permission in the QuickEntry controller when creating new timesheets. Authenticated users with view_other_timesheet and edit_other_timesheet permissions can create timesheet records for team members by submitting the QuickEntry form, bypassing authorization checks enforced elsewhere.	8.8	More Details
CVE-2026-82450	BookStack before 26.05.4 contains a remote code execution vulnerability in the portable ZIP import functionality that allows users with Import Content and Create Books permissions to upload a PHP polyglot file as a book cover. Attackers can bypass image extension validation by embedding a PHP file with a .php filename in the ZIP archive, which is stored in the public web root and executed by unauthenticated requests.	8.8	More Details
CVE-2026-80576	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: reject oversized IBs with per-ring packet limits On GFX rings, amdgpu_cs_p2_ib() passed user-supplied ib_bytes through to ib->length_dw without a limit, while ring_emit_ib() encodes length into packet fields. Oversized values can corrupt adjacent control bits and destabilize command submission. Add a per-ring IB packet size limit helper and reject command submissions exceeding the corresponding dword limit before IB allocation. Use the documented 20-bit limit for GFX/compute/SDMA/VPE, and apply the MM fallback limit for other ring types. (cherry picked from commit 7f48fa2cf62e3fa6c9c3870aa74988f773247e52)	8.8	More Details
CVE-2026-26899	An issue was discovered in luci-app-https-dns-proxy on OpenWrt PR #15 (< 2026-01-17). The setInitAction function in /usr/libexec/rpcd/luci.https-dns-proxy allows authenticated users to execute arbitrary shell commands via shell metacharacters in the name parameter	8.8	More Details
CVE-2026-	Skyvern before 1.0.45 contains a sandbox escape vulnerability in TextPromptBlock that renders prompts twice, first through a sandboxed Jinja environment and then through an unsandboxed environment.	8.8	More

82447	Attackers can inject malicious Jinja template syntax through workflow parameters or upstream block output to execute arbitrary code with server process privileges.		Details
CVE-2026-75339	The storage endpoint /storage/upload of cjbi admin3 v3.0.0 are missing permission checks. /Any logged-in user can upload arbitrary files, and any anonymous attacker can download them.	8.8	More Details
CVE-2026-55521	Yamcs is a mission control framework. Prior to 5.12.8 and 5.13.2, Yamcs omits authorization checks in IndexesApi.listPacketIndex, IndexesApi.listEventIndex, Cop1Api.disable, Cop1Api.resume, Cop1Api.initialize, Cop1Api.updateConfig, and TimeApi.setTime. An authenticated low-privilege user can read packet and event index metadata without ObjectPrivilegeType.ReadPacket, alter COP-1 link state without SystemPrivilege.ControlLinks, and manipulate simulation time. These operations can disclose telemetry metadata, disrupt telecommand handling, and affect system integrity and availability. This issue is fixed in versions 5.12.8 and 5.13.2.	8.8	More Details
CVE-2026-55485	Piccolo Admin is an admin interface and content management system for Python, built on top of Piccolo. Prior to 1.14.0, piccolo_admin/endpoints.py uses superuser_validators to block PUT, PATCH, DELETE, and POST requests by non-superusers but permits GET requests to configured user and session tables, while piccolo_api/session_auth/tables.py exposes SessionsBase.token because the token column is not secret. In deployments that add the Sessions and User tables to create_admin, a non-superuser administrator can call GET /api/tables/sessions/, obtain another user's live session token, replay it as the Cookie id value to impersonate a superuser, and permanently set superuser to true on the attacker's own row. This issue is fixed in version 1.14.0.	8.8	More Details
CVE-2026-80672	In the Linux kernel, the following vulnerability has been resolved: ntfs: fix u16 truncation of restart-area length check ntfs_check_restart_area() validates that the $LogFile restart area and its trailing log client record array fit within the system page size: u16 ra_ofs, ra_len, ca_ofs; ... ra_len = ca_ofs + le16_to_cpu(ra->log_clients) * sizeof(struct log_client_record); if (ra_ofs + ra_len > le32_to_cpu(rp->system_page_size) || ...) return false; ra_len is u16, but the right-hand side is computed in size_t (sizeof(struct log_client_record) == 160). Both ca_ofs and log_clients come straight from the on-disk restart area. With an on-disk log_clients of 410 the product 410 * 160 = 65600; adding ca_ofs and storing into the u16 ra_len truncates modulo 65536 (e.g. ca_ofs 64 gives ra_len 128), so the "fits in the page" check passes even though the client array described by log_clients extends far beyond the page. ntfs_check_log_client_array() then walks the array bounded only by the on-disk log_clients count: cr = ca + idx; if (cr->prev_client != LOGFILE_NO_CLIENT) ... For log_clients 410 it dereferences records up to ca + 409 * 160, ~64 KiB past the kvzalloc(system_page_size) restart-page buffer -- an out-of-bounds read of attacker-controlled extent, reachable when a crafted NTFS image is mounted (load_and_check_logfile() at mount time). This is the in-kernel analogue of CVE-2022-30789, fixed in the ntfs-3g userspace driver but never in this revived classic driver. Compute the restart-area length in a u32 so the existing bounds check rejects an over-large client array instead of being defeated by the truncation. Widen ra_ofs and ca_ofs to u32 as well: both are loaded from __le16 on-disk fields and every comparison already promotes to int/size_t, so this changes no result and keeps the declaration uniform.	8.8	More Details
CVE-2026-75419	go-wind-cms (GoWind) before 1.0.0 has a missing authorization vulnerability. The NewAuthorizer() function in app/admin/service/internal/data/data.go and app/app/service/internal/data/data.go returns a no-op authorization engine (noop.State{}), so the authz middleware always allows requests. Any authenticated user (regardless of role or tenant) can invoke administrative APIs such as deleting users, resetting passwords, and creating tenants.	8.8	More Details
CVE-2026-80724	In the Linux kernel, the following vulnerability has been resolved: ptp: vmclock: prevent read-only mappings from becoming writable vmclock_miscdev_mmap() rejects writable mappings of the shared vmclock ABI page with -EROFS, but leaves VM_MAYWRITE set. Userspace can map the page read-only and then upgrade it to writable with mprotect(), after which the guest can corrupt the host-written timekeeping data (sequence counter, UTC time, TSC offset) that the vmclock ABI defines as read-only. Clear VM_MAYWRITE on the read-only path so the mapping cannot be upgraded, as i915 does for its read-only objects and as fixed in drm/vc4 (CVE-2026-68445) and drm/panthor (CVE-2024-53071).	8.8	More Details
CVE-2020-15876	An issue was discovered in LibreNMS 1.65. A remote authenticated attacker with normal privileges can extract all the information from the LibreNMS database via a SQL injection in the sort parameter in the /ajax_table.php API endpoint. This affects address-search.inc.php, alertlog.inc.php, arp-search.inc.php, as-selection.inc.php, bills.inc.php, device_mibs.inc.php, device_oids.inc.php, edit-ports.inc.php, eventlog.inc.php, inventory.inc.php, ix-list.inc.php, ix-peers.inc.php, mempool-edit.inc.php, mempool.inc.php, mibs.inc.php, poll-log.inc.php, processor-edit.inc.php, processor.inc.php, routing-edit.inc.php, sensors-common.inc.php, storage-edit.inc.php, storage.inc.php, tnmsneinfo.inc.php, and toner.inc.php (in includes/html/table).	8.8	More Details
	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: SCO: give the socket its own sco_conn reference sco_conn_del() drops a reference it does not own. It takes one transient reference via sco_conn_hold_unless_zero() and releases it with the sco_conn_put() that follows sco_sock_hold(); the additional put in the !sk branch releases a second one: conn = sco_conn_hold_unless_zero(conn); ... sk = sco_sock_hold(conn); sco_conn_unlock(conn); sco_conn_put(conn); if (!sk) { sco_conn_put(conn); return; } When close() races the controller's Disconnection Complete, sco_chan_del() clears conn->sk and drops the socket's reference while sco_conn_del() is running. sco_conn_del() then sees sk == NULL, its own put drops the count to zero and frees the conn, and the second put writes to the freed kref: BUG: KASAN: slab-use-		

CVE-2026-80683	after-free in sco_conn_put.part.0+0x1a/0x190 Write of size 4 at addr ffff8881099dec74 by task kworker/u17:3/413 Workqueue: hci1 hci_rx_work Call Trace: sco_conn_put.part.0+0x1a/0x190 hci_disconn_complete_evt+0x1ee/0x3e0 hci_event_packet+0x54a/0x650 hci_rx_work+0x321/0x3d0 Allocated by task 413: sco_conn_add+0x72/0x1a0 sco_connect_cfm+0x88/0x670 Freed by task 413: sco_conn_del.isra.0+0x3f/0xf0 hci_disconn_complete_evt+0x1ee/0x3e0 refcount_t: underflow; use-after-free. The root cause is that the socket stores the connection without holding a reference of its own. __sco_chan_add() does: sco_pi(sk)->conn = conn; so the socket borrows whatever reference its caller happened to hold, and the callers paper over that with ad-hoc holds and puts. Give the socket a counted reference instead: __sco_chan_add() takes one and it is released together with the channel (sco_chan_del()) and in sco_sock_destruct(). With the socket holding its own reference, sco_conn_del() no longer needs the extra put and the redundant hold in sco_conn_ready() goes away. Making the socket own its reference means the connection is now actually freed on the error paths of sco_connect() where it used to leak, which in turn runs sco_conn_free() and its hci_conn_drop(conn->hcon). To keep the hci_conn accounting balanced, make that ownership explicit as well: sco_conn_add() consumes one hci_conn reference and the sco_conn owns it for its lifetime. sco_connect() hands over the reference returned by hci_connect_sco() and no longer drops it on the error paths; sco_connect_cfm(), which is not given a reference, takes one with hci_conn_hold() before handing it to sco_conn_add() (and drops it again if the allocation fails); and the explicit hci_conn_hold() in sco_conn_ready() is removed. Every reference then has a single, clear owner.	8.8	More Details
CVE-2026-80547	In the Linux kernel, the following vulnerability has been resolved: s390/vfio_ccw: Implement a crw lock Unlike the channel_program struct, which covers synchronous I/O submissions and asynchronous interrupts, the CRW region relies exclusively on asynchronous events coming from hardware. Implement a lock to manage the list of those payloads, to ensure they are read cohesively.	8.8	More Details
CVE-2026-80548	In the Linux kernel, the following vulnerability has been resolved: s390/vfio_ccw: Selectively expand io_mutex The io_mutex was defined to serialize the io_regions, but then has also sort of been associated with the I/O themselves because of the close relationship they share. With the handful of races that are possible, the choices are either to: A) expand the scope of io_mutex to close these remaining windows, or B) reduce the scope of io_mutex to just io_region, and introduce a new lock mechanism for the remaining I/O resources This patch implements A, since B brings with it a lot more interactions that would need to be tracked and kept in a correct hierarchy. It also takes advantage of the workqueue element for cp_free() that now gets called out of fsm_notoper(), which could be invoked out of an interrupt context and thus cannot acquire a mutex itself.	8.8	More Details
CVE-2026-80721	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: ISO: ensure no dangling hcon references in iso_conn After iso_conn_del(), ISO sockets should not dereference the hcon any more. Currently, clearing iso_conn::hcon relies on iso_conn_del() releasing the last reference to the iso_conn. Simplify this by explicitly clearing conn->hcon in iso_conn_del(), to avoid more complex reasoning on races about who holds the last reference.	8.8	More Details
CVE-2026-81579	In WibuKey for Windows before version 6.71, an untrusted pointer dereference in the WibuKey2_64.sys kernel driver for 64-bit Windows allows an attacker to exploit a write-what-where primitive, enabling local privilege escalation. This can be leveraged to execute arbitrary code, run an administrator shell, or gain full control over the system.	8.8	More Details
CVE-2026-81625	A remote attacker with user privileges may use a malicious or compromised NASL vulnerability test (VT) on the affected products to trigger a stack buffer overflow and gain full access on the compromised system.	8.8	More Details
CVE-2026-80553	In the Linux kernel, the following vulnerability has been resolved: s390/vfio_ccw: Cancel existing workqueues The initialization of the io_work and crw_work workqueues begs the question of whether they should be un-initialized. Add the corresponding cleanup tags in _release_dev to ensure work isn't dispatched after the private struct is free'd.	8.8	More Details
CVE-2026-79744	MCPHub is a unified hub for centrally managing and dynamically orchestrating multiple MCP servers/APIs into separate endpoints with flexible routing strategies. Prior to version 1.0.29, MCPHub's PUT /api/system-config endpoint (handler updateSystemConfig) performs no authorization check. It is protected only by the app-wide authentication middleware and a rate limiter — it never inspects req.user.isAdmin. This issue has been patched in version 1.0.29.	8.8	More Details
CVE-2026-81532	A user able to submit SQL through an application using the MongoDB Connector for BI ODBC driver can supply a positioned-cursor statement whose cursor name exceeds the size of an internal fixed-length buffer. Because the name length is not bounded before the driver builds its diagnostic message, memory adjacent to that buffer is overwritten with user-supplied content. This can terminate the hosting application process and may allow unintended code to run within it.	8.8	More Details
CVE-2026-80552	In the Linux kernel, the following vulnerability has been resolved: s390/vfio_ccw: Ensure index for read/write regions are within range The introduction of the capability chain rightly clamped the region indexes to the range of the capabilities itself, but neglected to do so for the existing read/write regions which should also be enforced.	8.8	More Details
CVE-2026-81581	Improper validation of memory boundaries in WibuKey64.sys of WibuKey up to 6.70 for Windows can be exploited by an attacker by setting the pointers outside the scope of the program. This usually results in a denial of service, yet we cannot rule out the possibility of exploits that can cause Remote Code Execution and Privilege Escalation (since the driver runs with system privileges).	8.8	More Details

CVE-2025-56798	Cross-Site Request Forgery (CSRF) vulnerability in Lime Technology, Inc.'s Unraid OS version 6.12.14 and earlier allows remote attackers to escalate privileges via the Unraid authentication cookie's lax same-site policy.	8.8	More Details
CVE-2026-83497	Unrestricted deserialization of untrusted data in the cursor pagination component in the OpenSearch SQL plugin allows a remote authenticated user with basic read/search permissions to execute arbitrary code on the server by sending a crafted cursor parameter to the plugins/sql endpoint.	8.8	More Details
CVE-2026-72984	Access of resource using incompatible type ('type confusion') in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	8.8	More Details
CVE-2020-15878	An issue was discovered in LibreNMS 1.65. A remote authenticated attacker with normal privileges can extract all the information from the LibreNMS database via a SQL injection in the address parameter in the /ajax_table.php API endpoint.	8.8	More Details
CVE-2026-82807	A vulnerability was determined in ieungSoft Ultra RAMDisk Pro 1.82. This issue affects some unknown processing in the library URDSCSI.sys of the component Kernel Driver. This manipulation causes improper privilege management. The attack needs to be launched locally. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2026-47665	Penpot is an open-source design and prototyping platform. In versions up to and including 2.14.3, Penpot is vulnerable to stored cross-site scripting through file comments, whose content is stored as raw text and rendered into the page with innerHTML without any sanitization. Because the backend applies only a length check and the frontend writes comment content directly through innerHTML, any team member who can comment on a shared file can embed HTML such as an image error handler or script that executes in the browser of every other collaborator. The attack is passive: any user who opens the comments panel on the affected file triggers script execution on the Penpot origin, allowing theft of session cookies, actions performed as the victim, and access to their files and projects. This issue is fixed in version 2.15.3.	8.7	More Details
CVE-2026-82466	Rodauth before 2.46.0 contains an authentication bypass vulnerability in the webauthn_login route that allows logged-in users to authenticate as any other account. Attackers can exploit improper account resolution logic that falls back to session account identifiers instead of validating the credential binding to complete authentication as arbitrary users.	8.7	More Details
CVE-2026-77693	The Order Tip for WooCommerce WordPress plugin before 1.6.0 does not check the capability of the user requesting a file deletion, nor does it restrict which path may be deleted, allowing users with the Shop Manager role and above to delete arbitrary files on the server, which could lead to the site being taken over.	8.7	More Details
CVE-2026-81091	The proxy middleware in mcp-use's inspector forwards requests to a destination the caller names. mountMcpProxy in libraries/typescript/packages/inspector/src/server/proxy/mcp-proxy.ts read the target from the X-Target-URL header or the __mcp_target parameter and proxied to it without inspecting the host, so loopback, link-local and private addresses were all accepted, as were names that resolve to them, and the validation was not reapplied to a redirect the destination returned. A caller could therefore make the server issue requests to addresses reachable only from the host it runs on and read the responses. The current code calls isSafeProxyTarget, which checks the resolved address against private, loopback and link-local ranges before proxying and bounds the number of redirects followed.	8.6	More Details
CVE-2026-55848	mapfish-print is a component of MapFish for printing templated cartographic maps. Prior to 3.28.30, 3.30.32, 3.31.24, 3.33.16, and 4.0.5, MapFish Print accepts an attacker-controlled GML layer url in requests to the /api/print3/print endpoint and fetches XML parsed by core/src/main/java/org/mapfish/print/map/geotools/GmlLayer.java without disabling external entities and external DTDs. A remote XML document and DTD can expand a local file entity, and the resulting content can be exposed through the GML parsing and error path. This allows unauthenticated attackers to read files such as operating-system account data, Kubernetes service-account tokens, and certificates. Replacing the file entity target with an internal HTTP endpoint also permits server-side request forgery. This issue is fixed in versions 3.28.30, 3.30.32, 3.31.24, 3.33.16, and 4.0.5.	8.6	More Details
CVE-2026-16061	The Rest Routes WordPress plugin through 5.5.5 does not sanitize and validate a value taken from the URL of one of its public REST routes before using it in a SQL query, allowing unauthenticated attackers to perform SQL injection attacks.	8.6	More Details
CVE-2026-82286	gpt-crawler through 1.5.1 fails to validate the outputFileName parameter in the POST /crawl endpoint, allowing unauthenticated attackers to write arbitrary files to any filesystem path. Attackers can supply absolute paths or parent-directory segments to overwrite existing files with content sourced from attacker-controlled URLs.	8.6	More Details
CVE-2026-54511	LogTape is an unobtrusive logging library. Prior to 1.3.11, 2.0.14, and 2.1.5, the @logtape/syslog package's escapeStructuredDataValue() function in packages/syslog/src/syslog.ts does not neutralize C0 control characters from U+0000 through U+001F in structured data values, and formatStructuredData() inserts property keys without validating the RFC 5424 SD-NAME grammar. When includeStructuredData is true, an attacker-controlled newline can terminate an RFC 6587 non-transparent TCP syslog frame and make following bytes appear as a forged RFC 5424 record, while a key containing a closing bracket or other forbidden character can terminate or corrupt the structured-data element. Applications that forward attacker-controlled property values or keys can therefore allow forged records with arbitrary hosts, applications, process identifiers, facilities, or severity levels, undermining downstream collector and SIEM	8.6	More Details

	integrity. This issue is fixed in versions 1.3.11, 2.0.14, and 2.1.5.		
CVE-2026-27330	Unauthenticated Broken Access Control in Mobile App for WooCommerce <= 0.4.62 versions.	8.6	More Details
CVE-2026-81573	If CodeMeter Runtime before 8.41a or 9.10 is configured as a server, the configuration command handler does not enforce network- origin restrictions. Commands intended only for local or same-network clients can therefore be executed by arbitrary remote peers. An attacker can read potentially sensitive configuration data and overwrite selected values in Server.ini. This does include the hash of the credentials for the CodeMeter WebAdmin, enabling WebAdmin takeover.	8.6	More Details
CVE-2026-80590	In the Linux kernel, the following vulnerability has been resolved: inet: frags: strip GSO state from fragments before reassembly A virtio_net_hdr (tun/tap, or AF_PACKET with PACKET_VNET_HDR) can mark an IPv4 or IPv6 fragment as GSO; nothing relates gso_type to frag_off. inet_frag_reasm_prepare()/inet_frag_reasm_finish() keep the first fragment's skb as the head of the reassembled datagram, including its shinfo->gso_size/gso_type/gso_segs, and chain the remaining fragments on frag_list with whatever linear/paged layout they arrived with. After ip_defrag() (ip_local_deliver(), nf_defrag_ipv4, ...) the reassembled skb therefore still claims to be GSO (SKB_GSO_DODGY), and the next software segmentation point - udp_rcv_segment() on local delivery, validate_xmit_skb(), or the ip_finish_output_gso() slow path - hands it to skb_segment(). skb_segment()'s frag_list walk assumes GRO-shaped input and hits one of its BUG_ON()s. Two writes to a tap by an unprivileged user in its own userns are enough: kernel BUG at net/core/skbuff.c:4899! Oops: invalid opcode: 0000 [#1] SMP KASAN NOPTI CPU: 0 UID: 1000 PID: 82 Comm: poc Not tainted 7.2.0-pentest+ #2 RIP: 0010:skb_segment+0x20ca/0x48b0 Call Trace: <TASK> __udp_gso_segment+0x29a/0x27d0 udp4_ufo_fragment+0x458/0x6c0 inet_gso_segment+0x429/0x1340 skb_mac_gso_segment+0x233/0x4f0 __skb_gso_segment+0x308/0x660 udp_queue_rcv_skb+0x440/0xad0 udp_unicast_rcv_skb+0xc7/0x2c0 udp_rcv+0x16ce/0x2260 ip_protocol_deliver_rcu+0x197/0x2d0 ip_local_deliver+0x430/0x690 ip_rcv+0x16f/0x1f0 __netif_receive_skb_one_core+0x15e/0x1c0 __netif_receive_skb+0x1e/0x110 netif_receive_skb+0xf6/0x5c0 tun_rx_batched.isra.0+0x3ab/0x790 tun_get_user+0x17c3/0x3550 tun_chr_write_iter+0xba/0x1b0 vfs_write+0x646/0x1130 </TASK> Kernel panic - not syncing: Fatal exception in interrupt This runs with BH disabled, so it is a panic rather than an oops. The same is reachable with CAP_NET_RAW in a netns where a defrag point precedes a GSO point, and from a guest whose VMM forwards virtio_net_hdr to a tap. The SKB_GSO_DODGY frag_list checks added by commit 3dcbdb134f32 ("net: gso: Fix skb_segment splat when splitting gso_size mangled skb having linear-headed frag_list") and by commit 9e4b7a99a03a ("net: gso: fix panic on frag_list with mixed head alloc types") do not cover it: page-backed heads skip them, and kmalloc heads skip them when gso_size == skb_headlen(head), which the sender controls. An skb entering a frag queue is an IP fragment by definition and cannot legitimately carry GSO state: GRO does not merge fragments and the stack segments before it fragments, so only untrusted sources are affected. This has been reachable since commit f43798c27684 ("tun: Allow GSO using virtio_net_hdr"), the first path that let userspace attach GSO metadata to an IP fragment. Reset the GSO fields of every fragment as it is queued, in inet_frag_queue_insert(), which IPv4, IPv6, nf_conntrack_reasm and 6lowpan reassembly share; then neither the head nor the frag_list members of the reassembled skb carry them (the members matter too: the ip_do_fragment()/ip6_fragment() fast paths send them out as they are). The head may remain CHECKSUM_PARTIAL; that is already accepted on receive and resolved by skb_checksum_help() in ip_do_fragment()/ip6_fragment() on forward. Tested on top of net.git (dc4b95b8fee9), x86_64: the tap reproducer above, two further IPv4 frag_list geometries that reach BUG_ON(i >= nfrags) and BUG_ON(!list_skb->head_frag), and an IPv6 fragment-header variant (udp6_ufo_fragment()) each panic the unpatched kernel; with this patch all four datagrams are delivered intact and nothing is logged.	8.6	More Details
CVE-2026-82641	keploy versions 3.1.0 through 3.6.25 bind the agent control-plane HTTP server to all interfaces without authentication, exposing endpoints that stream TLS session keys and traffic data. Attackers can access the /agent/pcap/keylog endpoint to retrieve NSS keylog lines and decrypt recorded TLS traffic, or invoke /agent/stop and /agent/storemocks to manipulate recording sessions.	8.6	More Details
CVE-2026-81093	The get-html-skeleton tool fetched a URL the caller supplied after checking only its syntax. The handler in src/tools/common/get_html_skeleton.ts validated the url argument with isValidHttpUrl from src/utils/generic.ts, which confirmed the string began with an http or https scheme and parsed as a URL and inspected neither the host name nor the address it resolves to. Loopback, link-local and private ranges therefore passed, including the address cloud providers use to serve instance metadata. The unchecked URL was handed to the web-browser actor and the fetched document was returned in the tool response, so any caller of the MCP server could make it request an endpoint reachable only from the host and read the result, including instance credentials. Version 0.9.12 removes the tool.	8.6	More Details
CVE-2026-82645	AVideo (current commit e01e41ecc and earlier) exposes stream credentials through the plugin/Live/view/Live_restreams/getLiveKey.json.php endpoint. Supplying a 'token' request parameter waives both the Live::canRestream() access gate and the restream ownership check, causing the endpoint to return any restream's stream_key and stream_url (credentials for external platforms such as YouTube, Facebook, and Twitch) without authentication. The token is merely encryptString() of an integer id with no user binding, expiry, or authentication tag. Because encryption uses AES-256-CBC with a deterministic IV and no MAC, and because intval() accepts any string beginning with a digit, an unauthenticated attacker can forge valid tokens using the public encryption oracle in view/url2Embed.json.php, disclosing arbitrary users' stream credentials.	8.6	More Details

CVE-2026-81027	one-api gates one of its two channel-pinning paths and not the other. middleware/auth.go permits a request to name a specific channel either through a suffix on the API key or through a URL path parameter. The suffix path is reached only after model.IsAdmin succeeds and otherwise rejects the caller, while the path-parameter branch sets the selected-channel value from c.Param("channelid") with no role check at all. The route carrying that parameter sits behind token authentication only, so any account holding a valid API token reaches it. The value flows to the distributor, which loads the channel by integer identifier with no scoping to the caller's user or group, and then sets the outbound Authorization header to that channel's stored key and directs the request at the channel's base URL. A low-privilege account can therefore pin any channel by incrementing an identifier, causing the server to make upstream requests bearing an operator-configured provider key the account was never granted, and bypassing both the per-group restriction and the channel's model allowlist.	8.5	More Details
CVE-2026-32550	Subscriber SQL Injection in Kadence Shop Kit <= 3.0.6 versions.	8.5	More Details
CVE-2026-32564	Subscriber SQL Injection in ACPT (Pro) - Custom Post Types Plugin for WordPress <= 2.0.63 versions.	8.5	More Details
CVE-2026-78285	Subscriber SQL Injection in Like Button Rating <= 2.6.61 versions.	8.5	More Details
CVE-2026-55108	KubeVela is an open source application delivery platform. Prior to 1.9.14, from 1.10.0-alpha.1 until 1.10.9, and from 1.11.0-alpha.1 until 1.11.0-alpha.4, the Terraform remote configuration loader in pkg/controller/utils/capability.go, GetTerraformConfigurationFromRemote, clones a repository supplied through a core.oam.dev/v1beta1 ComponentDefinition and follows repository-controlled variables.tf or main.tf symlinks. A user with permission to create or update ComponentDefinition objects can point variables.tf to /dev/zero through terraform.path, after which os.Stat and os.ReadFile follow the link and read an unbounded stream before ParseTerraformVariables or HCL parsing can reject the content. The read can exhaust memory, OOM-kill the cluster-wide vela-core controller, cause repeated Pod restarts, and pressure node memory when no effective container limit is configured. This issue is fixed in versions 1.9.14, 1.10.9, and 1.11.0-alpha.4.	8.5	More Details
CVE-2026-82227	Contributor SQL Injection in WPBulky <= 1.2.2 versions.	8.5	More Details
CVE-2026-81287	Subscriber SQL Injection in Charitable <= 1.8.12.1 versions.	8.5	More Details
CVE-2026-81277	Contributor SQL Injection in Suggestion Engine for WooCommerce <= 2.0.11 versions.	8.5	More Details
CVE-2026-80653	In the Linux kernel, the following vulnerability has been resolved: scsi: hisi_sas: Add slave_destroy interface for v3 hw WARNING is triggered when executing link reset of remote PHY and rmmod SAS driver simultaneously. Following is the WARNING log: WARNING: CPU: 61 PID: 21818 at drivers/base/core.c:1347 __device_links_no_driver+0xb4/0xc0 Call trace: __device_links_no_driver+0xb4/0xc0 device_links_driver_cleanup+0xb0/0xfc __device_release_driver+0x198/0x23c device_release_driver+0x38/0x50 bus_remove_device+0x130/0x140 device_del+0x184/0x434 __scsi_remove_device+0x118/0x150 scsi_remove_target+0x1bc/0x240 sas_rphy_remove+0x90/0x94 sas_rphy_delete+0x24/0x3c sas_destruct_devices+0x64/0xa0 [libsas] sas_revalidate_domain+0xe4/0x150 [libsas] process_one_work+0x1e0/0x46c worker_thread+0x15c/0x464 kthread+0x160/0x170 ret_from_fork+0x10/0x20 ---[end trace 71e059eb58f85d4a]--- During SAS phy up, link->status is set to DL_STATE_AVAILABLE in device_links_driver_bound, then this setting influences __device_links_no_driver() before driver rmmod and caused WARNING. Add the slave_destroy interface to make sure link is removed after flush workque.	8.4	More Details
CVE-2026-80574	In the Linux kernel, the following vulnerability has been resolved: Input: focaltech - fix array out-of-bounds in focaltech_process_rel_packet Make finger2 (and also finger1) unsigned, so that if the finger index in the packet is 0 then subtracting 1 creates an array index which overflows above the existing check for FOC_MAX_FINGERS, as the existing comment says it should, instead of writing to state->fingers[-1].	8.4	More Details
CVE-2026-80536	In the Linux kernel, the following vulnerability has been resolved: xfs: bounds-check buffer log item's dirty bitmap xlog_recover_do_reg_buffer() replays each dirty region described by a buffer log item's bitmap into the buffer read for that item: memcpy(xfs_buf_offset(bp, (uint)bit << XFS_BLF_SHIFT), item->ri_buf[i].iov_base, nbits << XFS_BLF_SHIFT); The destination offset (bit/nbits, from the logged dirty bitmap) and the buffer size (from the logged blf_len) are both attacker-controlled and otherwise unrelated, yet the only thing bounding the copy is an ASSERT(), which compiles away on production kernels. A crafted image logging a small blf_len together with a bitmap bit past the end of that buffer drives the memcpy() past the buffer's allocation, corrupting adjacent kernel heap during mount-time log recovery. This is reachable by anyone who can get a crafted image mounted -- the malicious-filesystem threat model XFS already guards against elsewhere. Turn the ASSERT() into a real XFS_IS_CORRUPT() check that aborts recovery of the buffer with -EFSCORRUPTED, consistent with the validate-and-fail idiom already used in xlog_recover_do_inode_buffer() and xfs_dquot_item_recover.c. xlog_recover_do_reg_buffer() therefore becomes STATIC int and its three callers propagate the error. Found and confirmed with KASAN on a CONFIG_XFS_DEBUG=n build: the crafted image trips a slab-out-of-bounds write before this change and fails	8.4	More Details

	recovery cleanly with -EFSCORRUPTED after it.		
CVE-2026-80712	In the Linux kernel, the following vulnerability has been resolved: spi: spi-qpic-snand: write the feature value before executing SET_FEATURE qcom_spi_send_cmdaddr() programs NAND_FLASH_CMD/NAND_EXEC_CMD and submits the descriptors, which makes the controller execute the command immediately. For SPINAND_SET_FEATURE the value to be written is only placed into NAND_FLASH_FEATURES afterwards, by qcom_spi_io_op(), in a second submission - so the chip is programmed with whatever that register happened to hold from a previous operation, and the intended value is only applied by the *next* SET_FEATURE. Measured on a TP-Link Archer AX55 v1 (IPQ5018, ESMT F50L1G41LB): writing 0x40 to the configuration register (0xb0) leaves the chip at 0x00, and the subsequent write of 0x00 leaves it at 0x40 - every write lands one operation late. This stayed unnoticed until v6.18 added SPI-NAND OTP support together with OTP entries for ESMT chips. spinand_otp_rw() enables OTP mode, reads, and disables it again, and mtd_otp_nvmem_add() does this during MTD registration. With the off-by-one, the "disable" write actually applies the previously requested value, so CFG_OTP_ENABLE ends up set: the chip stays in OTP mode, every subsequent array read returns the OTP area instead of the array (UBI reports an empty device) and all writes fail with -EIO because the OTP area is write protected. On this board that makes the whole flash unusable and the device unbootable. Write the feature value into NAND_FLASH_FEATURES as part of the same transaction, before NAND_EXEC_CMD. While at it, copy only the bytes the operation actually carries - the previous code dereferenced a 4-byte pointer on a one-byte buffer (spinand->scratchbuf). With this patch the flash contents read back bit-identical to a known-good dump of the same board taken under the vendor firmware (md5-verified across partitions), and writes work.	8.4	More Details
CVE-2026-80593	In the Linux kernel, the following vulnerability has been resolved: hwmon: (asus_atk0110) Check package count before accessing element atk_ec_present() walks the management group package returned by the GGRP ACPI method and, for each sub-package, reads its first element: id = &obj->package.elements[0]; if (id->type != ACPI_TYPE_INTEGER) without checking that the sub-package is non-empty. ACPICA allocates the element array with exactly package.count entries, so for a sub-package with a zero count this reads past the allocation. The sibling function atk_debugfs_ggrp_open() performs the same access but skips empty packages with a package.count check first. Add the same check to atk_ec_present() so a malformed firmware package cannot trigger an out-of-bounds read.	8.4	More Details
CVE-2026-80596	In the Linux kernel, the following vulnerability has been resolved: Input: ims-pcu - only expose sysfs attributes on control interface When the driver was converted to use the driver core to instantiate device attributes (via .dev_groups in the usb_driver structure), the attributes started appearing on all interfaces bound to the driver. Since the ims-pcu driver manually claims the secondary data interface during probe, the driver core automatically creates the sysfs attributes for that interface as well. However, the driver only supports these attributes on the primary control interface. Data interfaces lack the necessary descriptors and internal state to handle these requests, and accessing them can lead to unexpected behavior or crashes. Fix this by updating the is_visible() callbacks for both the main and OFN attribute groups to verify that the interface being accessed is indeed the control interface.	8.4	More Details
CVE-2026-81097	The execute_ruby tool is documented as a read-only Ruby sandbox and is enforced by a pattern denylist together with replacements for the process-spawning methods on Kernel. The pseudo-terminal library's spawn entry points are neither in the denylist nor replaced, so a normal tool call could reach them and start a shell, executing commands as the account running the server and outside the guarded methods. The denylist was introduced with the tool in 1.4.0 and never covered those entry points through 1.6.0. Version 1.6.1 restricts the requires the sandbox permits to a data-only list and blocks dynamic dispatch to execution entry points; 2.0.0 removes the tool.	8.4	More Details
CVE-2026-81683	openssl_encrypt (pip package openssl-encrypt) versions 1.4.8 and earlier store an mTLS client private key in cleartext within a world-readable (0644) SharedPreferences file via the desktop GUI's Settings screen 'combined certificate and private key' PEM field. A local attacker with file system access can read the exposed private key. Version 1.4.9 writes the PEM to a dedicated 0600 file, keeps only its path in SharedPreferences, and migrates/scrubs existing cleartext values.	8.4	More Details
CVE-2026-82862	Hulumi versions before v1.3.2 resolve the threat-model helper script from an unsafe root, allowing workspace files to shadow the intended helper script. Attackers can place malicious files in the workspace to execute arbitrary code during local skill execution.	8.4	More Details
CVE-2026-80713	In the Linux kernel, the following vulnerability has been resolved: io_uring: preserve task restrictions across exec Per-task restrictions apply to all rings created by a task. Once installed, they should not be dropped across exec. For a task that has used io_uring, the exec cancellation path calls __io_uring_free(). This frees both the task context and the per-task restriction, so a ring created after exec is unrestricted. Split task context cleanup into io_uring_free_tctx(), and use it from the exec cancellation path. Keep __io_uring_free() for final task cleanup, where both the context and restriction are released.	8.4	More Details
CVE-2026-80723	In the Linux kernel, the following vulnerability has been resolved: of: reserved_mem: prevent OOB when too many dynamic regions are defined On boot, fdt_scan_reserved_mem() saves each dynamically-placed /reserved-memory subnode into a local array of size MAX_RESERVED_REGIONS. If the device tree defines more than MAX_RESERVED_REGIONS dynamically-placed regions, fdt_scan_reserved_mem() writes past the end of the local array. Add a bounds check that logs an error and skips the excess regions, restoring the original behavior.	8.4	More Details
	In the Linux kernel, the following vulnerability has been resolved: s390/qeth: validate user buffer length in		

CVE-2026-80584	SNMP and ARP query ioctls qeth_snmp_command() and qeth_l3_arp_query() allocate a buffer sized by a user-supplied length (udata_len) without checking a lower bound, then set udata_offset to a fixed non-zero value and pass both to a reply callback. The callback bounds-checks the copy with if ((udata_len - udata_offset) < len) Both fields are u32, so a udata_len smaller than udata_offset makes the subtraction wrap and the check pass, and the following memcpy() writes past the allocation. A udata_len of 0 also yields ZERO_SIZE_PTR from kzalloc(), which the existing NULL check does not catch. Reject buffers smaller than udata_offset before allocating, so the callback subtraction can no longer underflow.	8.4	More Details
CVE-2026-80427	bestzip builds the argument list for the system zip utility without separating options from operands. The destination archive path and the caller-supplied source paths are passed to the child process with no -- delimiter between them, so any source entry beginning with a hyphen is interpreted by zip as an option rather than a file name. zip accepts -T to test the finished archive and -TT to name the command used to perform that test, so a source list containing those two entries and a command string causes zip to run that command through a shell once the archive has been written. An application that passes a file name or path it received from an untrusted source into the bestzip API therefore executes a command of the supplier's choosing. Versions 2.2.6 and 3.0.2 add the delimiter.	8.4	More Details
CVE-2026-80678	In the Linux kernel, the following vulnerability has been resolved: i2c: imx: Fix slave registration race and error handling In i2c_imx_reg_slave(), the slave pointer was assigned before pm_runtime_resume_and_get(). If pm_runtime_resume_and_get() failed, the error path returned without clearing i2c_imx->slave, leaving it non-NULL and causing all subsequent registration attempts to fail with -EBUSY. Additionally, because this driver uses a shared IRQ, the interrupt handler i2c_imx_isr() can execute concurrently and, after acquiring slave_lock, dereference i2c_imx->slave. The previous fix attempt added a lockless i2c_imx->slave = NULL on the error path, but that could race with the ISR under the lock and still cause a NULL pointer dereference. Fix both issues by deferring the assignment of i2c_imx->slave and i2c_imx->last_slave_event to after a successful resume, and by performing the assignment inside the slave_lock critical section. This guarantees that the slave pointer is never left stale on the error path and is always valid when observed by the interrupt handler.	8.4	More Details
CVE-2026-38820	openNDS before 11.0.0 is susceptible to unauthenticated OS command execution via shell command injection through the fas query parameter on the /opennds_preauth/ endpoint because of libopennds.sh.	8.3	More Details
CVE-2026-82021	Hermes Agent 0.18.2 prior to 0.19.0 contains a supply chain vulnerability in its bundled MCP catalog that allows a remote attacker to execute arbitrary code by compromising a third-party upstream repository referenced via a mutable branch rather than a pinned commit SHA. An attacker who compromises the upstream repository can propagate malicious code to every host that installs the affected catalog entry, with no further action required by the operator.	8.3	More Details
CVE-2026-82549	A vulnerability was identified in Linux Foundation Magma 1.9.0. This affects an unknown function of the component SecurityModeComplete Handler. Such manipulation leads to improper validation of integrity check value. The attack may be launched remotely. The exploit is publicly available and might be used.	8.3	More Details
CVE-2026-75871	GitLab has remediated a vulnerability in the GitLab AI Gateway component affecting all versions of the AI Gateway from 18.10 to 19.0.12, 19.1 to 19.1.7, and 19.2 to 19.2.2 that could have allowed an authenticated user with Duo Agent Platform access to redirect outbound model requests to an externally-controlled endpoint via a crafted inline flow configuration that overrides the HTTP Host header, resulting in disclosure of Google Cloud Vertex cloud service credentials and private signing keys.	8.2	More Details
CVE-2026-18904	IBM Langflow OSS 1.0.0 through 1.11.1 could allow a remote attacker to obtain sensitive information and inject unauthorized messages due to a namespace collision between user identifiers.	8.2	More Details
CVE-2026-80208	APITable through 1.13.0-beta.1 annotates both getUserHistories and closePausedUserAccount in InternalUserController with requiredLogin = false. ResourceInterceptor honours that annotation by returning before any session or API key is validated, and the nginx gateway shipped with the product proxies every /api request to the backend server, so both endpoints are reachable by any unauthenticated client that can reach the gateway. An attacker can POST to /api/v1/internal/getUserHistories to enumerate the accounts sitting in the 30-day cooling-off period that follows a deletion request, then POST to /api/v1/internal/users/{userId}/close for each one. The closure path clears the account's email address, phone number and nickname, cancels its space subscriptions, removes its space memberships and deletes its OAuth bindings, so the cooling-off window that exists to let a user reverse a deletion request is bypassed and the account cannot be recovered.	8.2	More Details
CVE-2026-19889	GitLab has remediated a vulnerability in the GitLab AI Gateway component affecting all versions of the AI Gateway from 18.9.0 to 19.0.12, 19.1 to 19.1.7, and 19.2 to 19.2.2 that could have allowed an authenticated user with Duo Agent Platform access to redirect model requests to an externally-controlled endpoint via crafted model metadata, resulting in the disclosure of Google Vertex AI or AWS Bedrock cloud service credentials.	8.2	More Details
CVE-2026-82234	SiYuan versions before v3.8.1 contain a server-side request forgery vulnerability in the http_request and web_fetch agent tools that perform DNS resolution only at guard time without validating the connect-time resolution. Attackers can use DNS rebinding to answer the guard resolution with a public IP and the connect resolution with a private or metadata IP, bypassing the SSRF defense to access cloud instance metadata and internal services.	8.2	More Details

CVE-2026-47877	Spring Security Authorization Server's default consent page renders user-controlled values without HTML entity encoding. Spring Security 7.1.0 Spring Security 7.0.0 - 7.0.6	8.2	More Details
CVE-2026-18794	The OpenRGB network protocol allows attackers to cause memory exhaustion and out-of-bounds memory reads and writes by passing inconsistent data.	8.2	More Details
CVE-2026-80549	In the Linux kernel, the following vulnerability has been resolved: s390/vfio_ccw: Move cp cleanup out of not operational The fsm_notoper() routine is called when the device has been lost, and is (by definition) no longer operational. Since this can happen asynchronously from the normal behavior of the driver, the cleanup may happen when holding other locks in the calling sequence (notably, the cio subchannel lock). Push the cleanup of the private->cp resources to a workqueue, where it can be done out from under that lock sequence and a future patch can safely manage the locking requirements.	8.2	More Details
CVE-2026-76548	The User Profile Builder WordPress plugin before 4.0.1 does not properly restrict its front-end file upload feature, granting unauthenticated visitors capabilities reserved to privileged roles. This allows them to list the site's media library and to modify unpublished posts, pages and media items belonging to other users.	8.2	More Details
CVE-2026-82473	KubeEdge CloudCore through 1.23.1 accepts node task status reports on its HTTPS server without authentication verification. Attackers can reach CloudCore on port 10002 to mark upgrade jobs as succeeded or failed, deceiving the control plane about node upgrade status and blocking further upgrade scheduling.	8.2	More Details
CVE-2026-81730	Dolibarr 9.0.0 through 23.0.4 saves inbound email attachments under the name supplied in the message's MIME headers without reducing it to a safe basename. The global saveAttachment() in htdocs/emailcollector/lib/emailcollector.lib.php builds $filepath = $path . $filename . '.' . $ext and hands it to file_put_contents(), and the private saveAttachment() in htdocs/emailcollector/class/emailcollector.class.php writes to $destdir.'/'.$filename; the name reaches both from the attachment's own getName() or getFilename() value by way of the record-join, create-ticket and create-project operations. A traversal sequence in the filename therefore survives intact, so any sender who can email a mailbox that an EmailCollector monitors, which is the module's ordinary use for a support or ticket inbox, can place attacker-controlled content outside the per-object attachment directory without holding a Dolibarr account. Under the hardened layout Dolibarr's SECURITY.md requires, with htdocs read-only, the write is confined to the documents tree and corrupts or forges other objects' documents; where htdocs is writable the same primitive reaches a web-executable path. Version 24.0.0 applies dol_sanitizePathName() and dol_sanitizeFileName() before the write.	8.2	More Details
CVE-2026-77538	A malicious actor with access to the network could exploit an Improper Access Control vulnerability found in UniFi Connect Application to escalate privileges within the UniFi Connect Application.	8.2	More Details
CVE-2026-18891	IBM Langflow OSS 1.0.0 through 1.11.1 could allow a remote attacker to execute arbitrary flows and access sensitive information due to improper authentication.	8.2	More Details
CVE-2026-82876	Phison PS3111-S11 controller firmware verifies RSA signatures using a public modulus embedded within the firmware image itself rather than anchored in immutable storage. Attackers can generate arbitrary RSA key pairs, sign modified firmware with the private key, embed the matching modulus in the signature segment, and the controller accepts the tampered firmware as valid.	8.2	More Details
CVE-2026-59316	Spring Authorization Server's default consent page renders user-controlled values without HTML entity encoding. When using the DefaultConsentPage, an attacker can craft an OAuth2 authorization request containing a malicious value that is stored server-side and later rendered unencoded in the default consent page presented to the end user. Spring Authorization Server 1.5.0 - 1.5.8 Spring Authorization Server 1.4.0 - 1.4.11	8.2	More Details
CVE-2026-81574	In CodeMeter Runtime before versions 8.41a and 9.10, the logger does not sanitize input strings in certain cases, allowing an attacker to inject printf-style format specifiers. This can be used to reliably crash CodeMeter and disclose sensitive information such as process memory and stack canaries. The attack works locally, for example by using cmu --set-proxy to set the proxy value, and remotely when combined with CVE-2026-81573 by setting General.ProxyServer and then triggering this vulnerability.	8.2	More Details
CVE-2026-80615	In the Linux kernel, the following vulnerability has been resolved: net: dst_metadata: fix false-positive memcpy overflow in tun_dst_unclone kmalloc_flex() in metadata_dst_alloc() sets __counted_by for the structure to the options_len, which is then initialized to zero. Later, we're initializing the structure by copying the tunnel info together with the options, and this triggers a warning for a potential memcpy overflow, since the compiler estimates that the options can't fit into the structure, even though the memory for them is actually allocated. memcpy: detected buffer overflow: 104 byte write of buffer size 96 WARNING: CPU: X PID: Y at lib/string_helpers.c:1036 __fortify_report skb_tunnel_info_unclone+0x179/0x190 geneve_xmit+0x7fe/0xe00 The issue is triggered when built with clang and source fortification. Fix that by doing the copy in two stages: first - the main data with the options_len, then the options. This way the correct length should be known at the time of the copy. It would be better if the options_len never changed after allocation, but the allocation code is a little separate from the initialization and it would be awkward and potentially dangerous to return a struct with options_len set to a non-zero value from the metadata_dst_alloc(). Another option would be to use ip_tunnel_info_opts_set(), but it is doing too many unnecessary operations for the use case here.	8.2	More Details

CVE-2026-80236	Efence developed by Thinking Software Technology has a SQL Injection vulnerability. Unauthenticated remote attackers can access file upload functionality and read database contents.	8.2	More Details
CVE-2026-59324	When an IntegrationFlow uses .fluxTransform() with an asynchronous/reordering fluxFunction that emits raw payloads, concurrent requests on the same FluxMessageChannel subscription have their reply headers (replyChannel, errorChannel, correlationId, any propagated security/tenant headers) copied from whichever message was most recently consumed upstream. Spring Integration 7.1.0 Spring Integration 7.0.0 - 7.0.5 Spring Integration 6.5.0 - 6.5.10 Spring Integration 6.4.0 - 6.4.12 Spring Integration 5.5.21 and earlier	8.2	More Details
CVE-2026-82285	bisheng through 2.6.0-fix2 contains a server-side request forgery vulnerability in the POST /api/v1/workflow/report/callback endpoint that lacks authentication and applies no URL scheme restrictions or host filtering. Unauthenticated attackers can supply arbitrary URLs to enumerate internal network services and cloud metadata endpoints, then retrieve captured responses from object storage using caller-supplied object names.	8.2	More Details
CVE-2026-77977	Ebyte gateway product's vendor configuration utility does not require authentication before allowing certain disruptive administrative actions when default credentials remain configured. An unauthenticated attacker on the adjacent network could reboot the device or restore factory settings, resulting in a loss of configuration and service availability.	8.1	More Details
CVE-2026-58092	In FreeBSD 15.0, the kernel structure used to represent user credentials changed: previously the primary group ID was stored in the first element of the array containing the list of supplementary group IDs, whereas now the primary group ID is stored in a dedicated field. This change was largely internal to the kernel and not user-visible. One function, group_is_primary(), was not properly updated as a part of this transition. This function is used by mac_do to determine the primary group ID of the credential after applying a transition rule, used when the rule target does not explicitly specify a group. As a result, with certain mac_do rules, it is possible for a credential switch to incorrectly set the primary group ID to the ID stored in the first element of the original credential's supplementary group array. If the list of supplementary groups is empty, this value will be 0, corresponding to the "wheel" group. For example, a rule such as "uid=1001>uid=1002" can be abused to set the primary group ID to 0 even if the process did not originally belong to group 0. Certain mac_do rules can be abused to set a process' group ID to 0. Note however, that the rule must apply to the caller in order for the bug to be triggered, e.g., given the ruleset "uid=1001>uid=1002", the user must have user ID 1001 in order to trigger the bug. Further, logged-in users will in general have a non-empty supplementary group list, in which case the bug can at worst be used to set the credential's first supplementary group ID as its primary group ID. Processes must explicitly remove themselves from all supplementary groups, using the privileged setgroups(2) system call, in order to exploit the bug to set 0 as the primary group ID. Since membership in group 0 is often used to enable controlled privilege escalation, the bug might be further exploitable to obtain root privileges, depending on the system configuration. For instance, a ruleset such as the following could be exploited by a process running as user 1001 and with an empty supplementary group list: "uid=1001>uid=1002;gid=0>uid=0".	8.1	More Details
CVE-2026-80192	@better-auth/sso before 1.6.27 (and before 1.4.8 in the 1.4.x line and before 1.7.0-rc.5 in the 1.7 prerelease line) contains two domain-ownership flaws. When domain verification is disabled, automatic organization assignment accepts unverified provider domains, allowing an authenticated organization owner/administrator to register an SSO provider for an arbitrary domain and have users with matching email domains added to the attacker's organization with default member permissions. When domain verification is enabled, a race condition between the verify-domain and update-provider endpoints can apply completed DNS proof to a different domain; combined with implicit account linking, this can link an attacker-controlled identity provider to an existing user account. Exploitation requires the SSO plugin (and, for the org-assignment path, the organization plugin) with the relevant configuration enabled.	8.1	More Details
CVE-2026-80645	In the Linux kernel, the following vulnerability has been resolved: rapidio/tsi721: prevent a bad dereference in tsi721_db_dpc() With a list_for_each() loop, if we don't find the item we are looking for in the list, then the loop exits with the iterator, which is "dbell" in this loop, pointing to invalid memory. This code uses the "found" variable to determine if we have found the doorbell we are looking for or not. However, the problem that the "found" variable needs to be set to false at the start of each iteration, otherwise after the first correct doorbell, then everything is marked as found. Reset the "found" to false at the start of the iteration and move the variable inside the loop.	8.1	More Details
CVE-2026-79746	MCPHub is a unified hub for centrally managing and dynamically orchestrating multiple MCP servers/APIs into separate endpoints with flexible routing strategies. Prior to version 1.0.31, when a bearer key with accessType: 'servers' (or 'custom') is used against a group route, isBearerKeyAllowedForRequest grants access to the entire group as long as any single server in that group appears in the key's allowedServers list — not only when every server the key is scoped to matches, and critically, without ever re-checking allowedServers again once the group-level connection is authorized. A key explicitly scoped to one specific server therefore also grants full access to every other server that happens to share a group with it, including servers the key was never authorized for. This issue has been patched in version 1.0.31.	8.1	More Details
CVE-2026-55228	Weblate is a web-based continuous localization platform used to manage software translations. In versions prior to 2026.7, the REST API did not properly enforce the scope of project- and workspace-scoped teams, allowing a user to submit invalid team configurations through the API. By assigning projects to a team via these unvalidated requests, a user could grant access to projects they were not authorized to see or manage. This could expose private projects and permit translation, repository, and project-management operations outside the user's intended permission scope. This issue is fixed in version 2026.7.	8.1	More Details

CVE-2026-81029	OpenMetadata accepts a caller-supplied post-authentication redirect target and appends the issued token to it. SamlLoginServlet reads the callback request parameter and stores it in the HTTP session without comparing it against any configured or registered destination, and the assertion consumer servlet later formats that stored value into a URL carrying the freshly issued JWT together with the account's email and name before sending the redirect. The OIDC and OAuth2 handler follows the same pattern with its own redirect parameter and the issued identity token. A request naming a destination the attacker controls therefore causes the server to deliver a valid token for whoever completes the login to that destination. Because the token authenticates API calls as that account, a user who follows such a link and authenticates hands over control of their account. Version 2.0.0 removes the caller-supplied callback parameter; no 1.x release validates it.	8.1	More Details
CVE-2026-82240	Budibase before 3.41.3 fails to validate app-scoped builder role assignments in the public user create and update endpoints, allowing an authenticated app-scoped builder to grant builder access to unrelated apps. Attackers can submit crafted requests to the user update API with builder.apps fields to escalate privileges and gain unauthorized builder access to other applications in the same tenant.	8.1	More Details
CVE-2026-32258	Winter is a free, open-source content management system (CMS) based on the Laravel PHP framework. From 1.2.10 through 1.2.12, authenticated backend users with the backend.manage_editor permission can store custom Markup Styles that are compiled by the LESS parser and rendered without sanitization on every backend page, allowing stored cross-site scripting. This issue is fixed in version 1.2.13.	8.1	More Details
CVE-2026-19718	The BlogVault Backup & Staging WordPress plugin before 6.65, MalCare WordPress Security Plugin WordPress plugin before 6.65, The WP Remote WordPress Plugin WordPress plugin before 6.65 do not prevent unauthenticated users from obtaining data derived from the secret that binds a site to its remote management service, and generate that secret with a weak pseudo-random number generator, allowing attackers to recover it and gain administrative access to the site.	8.1	More Details
CVE-2026-72001	Pangolin before 1.22.0 contains an authentication bypass vulnerability that allows unauthenticated attackers to access any protected resource by supplying an attacker-controlled URL parameter to the share-link authentication endpoint that omits the expected resource identifier from the token verification call. Attackers holding a single valid share link for any resource can authenticate against arbitrary resources across different organizations, bypassing all configured authentication methods including SSO, resource passwords, PIN codes, email allowlists, and header authentication.	8.1	More Details
CVE-2026-81036	Stalwart Mail Server does not compare an OAuth redirect target against any registered destination in its default configuration. The validation routine in crates/http/src/auth/oauth/registration.rs returns success immediately when the client-authentication requirement is disabled, and that requirement is false in the shipped settings, so the supplied redirect value is neither matched against a registered client nor otherwise constrained. The value is stored with the authorization code, and the login page reads it back and sends the browser to it with the code attached. A request naming a destination the attacker controls therefore delivers a valid authorization code there once the account holder authenticates, and because the token endpoint checks only that the redirect presented at exchange matches the one recorded with the code, the same party can exchange it for access and refresh tokens and read the account's mail.	8.1	More Details
CVE-2026-32257	Winter is a free, open-source content management system (CMS) based on the Laravel PHP framework. Prior to 1.2.13, custom CSS supplied through the Brand Settings Styles field by a backend user with the backend.manage_branding permission is compiled by the LESS parser and rendered without sanitization on every backend page, allowing stored cross-site scripting against backend users. This issue is fixed in version 1.2.13.	8.1	More Details
CVE-2026-56100	SpringBlade versions from 2.7.3 up to but not including 5.0.0 contain a privilege escalation vulnerability that allows authenticated attackers to create system administrator accounts by sending crafted POST requests to an unprotected internal Feign user-creation endpoint exposed via @RestController without authorization checks. Attackers can exploit the gateway's authentication filter, which only validates JWT parsing without verifying user roles or caller identity, and leverage a hardcoded JWT signing key embedded in publicly available JARs to forge tokens and escalate privileges from a low-privilege user to administrator, enabling cross-tenant data pollution and persistent backdoor access.	8.1	More Details
CVE-2026-61641	Wallos is an open-source, self-hostable personal subscription tracker. From version 4.0.0 to before version 4.9.6, Wallos's OIDC login links an incoming OIDC identity to an existing local account by matching the email claim alone, without verifying that the IdP marked that email as verified (email_verified). When Wallos is configured against an IdP that lets a user present an arbitrary or unverified email (multi-tenant IdPs, IdPs with open self-registration, or any IdP the attacker partly controls), an attacker with no Wallos account can authenticate with the admin's email and be logged in as the admin — full account takeover, no password needed. This issue has been patched in version 4.9.6.	8.1	More Details
CVE-2026-75458	The teacher-end interface POST /api/teacher/user/delete/{id} in XueZhiSi Open Source Exam System <= 3.9.0 contains a vertical privilege escalatio vulnerability. This interface accepts a user ID and then executes getUserById(id), setDeleted(true), updateByIdFilter() in sequence, without any validation of whether the current user has the authority to delete the target user. An authenticated teacher user (role=2) can delete an administrator account (role=3), constituting a vertical privilege escalation where a lower-privileged user performs a high-privileged operation.	8.1	More Details

CVE-2026-81035	Midday allows any member of a team to delete it. The delete procedure in apps/api/src/trpc/routers/team.ts authorises the caller with the team-access helper, which returns true for every row in the team-membership table irrespective of the role it records, and the data-layer function it calls re-checks the same helper and nothing else. The neighbouring procedures that remove or update a member in the same router each resolve the caller's role and refuse the request unless it is owner, so the check exists in the file and is not applied to deletion. Member is the role an invited user receives, so any invitee can remove the team and every record scoped to it, and the deletion enqueues the cleanup job with the stored bank-connection tokens, which the job then uses against the connected providers. The update procedure in the same router carries no role check either.	8.1	More Details
CVE-2026-82239	Budibase before 3.41.3 fails to enforce per-table role restrictions on the POST /api/datasources/query endpoint, allowing low-privilege BASIC users to read, create, update, or delete rows in any table regardless of configured permissions. Attackers with BASIC role can submit crafted query requests with target table identifiers to bypass table-level access controls and manipulate restricted data.	8.1	More Details
CVE-2026-82463	pac4j-core before 6.5.6 contains an authentication bypass vulnerability in CheckProfileTypeAuthorizer that reverses the profile type validation logic. Attackers can authenticate through a weaker client and access resources requiring a stronger profile type by satisfying generic profile checks.	8.1	More Details
CVE-2026-75020	Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') vulnerability in Apache APISIX. A caller who holds valid credentials for one entry in the LDAP directory can authenticate through APISIX as a consumer mapped to a different entry, one the plugin's configured scope was meant to keep out of reach. This issue affects Apache APISIX: from 2.11.0 through 3.17.0. Users are recommended to upgrade to version 3.18.0, which fixes the issue.	8.1	More Details
CVE-2026-82461	pac4j-oidc before 6.5.6 fails to verify access token signatures, issuers, audiences, or expiry when extracting Keycloak realm and client roles. Attackers can forge access tokens with administrative roles paired with valid ID tokens to bypass authorization checks in applications relying on pac4j role validation.	8.1	More Details
CVE-2026-82245	Budibase before 3.41.3 fails to enforce role-based authorization on license management endpoints, allowing any authenticated user to delete license keys or manipulate offline tokens. Attackers with basic user privileges can access /api/global/license/* endpoints to disable premium features and downgrade deployments for all users.	8.1	More Details
CVE-2026-54330	Ceph is an open-source distributed storage platform providing object, block, and file storage. In versions prior to 20.2.4 and 19.2.6, the Ceph Object Gateway (RGW) SigV4 handler does not reject requests that carry x-amz-* headers absent from the signed header set, allowing anyone holding a presigned URL to attach arbitrary unsigned x-amz-* headers that RGW will honor. AWS S3 requires every x-amz-* header on a SigV4 request to be signed and rejects requests bearing additional unsigned headers, but RGW validates only the headers listed in X-Amz-SignedHeaders and ignores any extra ones, so they take effect without being covered by the signature. By adding such headers to a presigned PUT URL, an attacker can grant themselves more capabilities than the URL's signer intended and escalate their privileges. This issue is fixed in versions 20.2.4 and 19.2.6.	8.1	More Details
CVE-2026-55065	Vikunja is an open-source self-hosted task management platform. From 0.24.6 until 2.4.0, DELETE /api/v1/projects/:project/views/:view permits an authenticated user to supply a view identifier from another project while authorizing only against an attacker-controlled project identifier. ProjectView.CanDelete in pkg/models/project_view_permissions.go does not establish that the view belongs to the path project, and ProjectView.Delete in pkg/models/project_view.go continues after the scoped project_views delete affects no rows. Its subsequent deletes select task_buckets and task_positions only by project_view_id, allowing cross-tenant destruction of Kanban assignments and ordering while leaving the victim view and tasks intact. This issue is fixed in version 2.4.0.	8.1	More Details
CVE-2026-82475	iFlytek astron-agent through 1.1.1 contains an authorization bypass vulnerability in the copyFlow endpoint that fails to validate workflow ownership. Authenticated attackers can enumerate workflow identifiers and overwrite other tenants' workflows or copy private workflows to read their definitions.	8.1	More Details
CVE-2026-82284	Quivr versions through 0.0.322 fail to validate chat ownership in the GET /chat/{chat_id}/history, DELETE /chat/{chat_id}, and POST /chat/{chat_id}/question/answer endpoints. Authenticated attackers can read other users' conversation histories including private knowledge base content, delete arbitrary chats, and inject fabricated messages into other users' conversations.	8.1	More Details
CVE-2026-59285	Spring for GraphQL applications are vulnerable to Unsafe Deserialization when processing paginated GraphQL queries. Spring for GraphQL 2.0.0 - 2.0.4	8.1	More Details
CVE-2026-59286	The GraphiQL page bundled with Spring for GraphQL loads JavaScript libraries from a public CDN, without Subresource Integrity checks. An attacker can inject malicious code in those scripts and execute arbitrary code on the browser loading the GraphiQL page. Spring for GraphQL 2.0.0 - 2.0.4 Spring for GraphQL 1.4.0 - 1.4.6 Spring for GraphQL 1.1.0 - 1.3.9 Spring for GraphQL 1.0.0 - 1.0.7	8.1	More Details
CVE-2026-75960	Rently Smart Home versions 20.1.0 and prior are vulnerable to an Insufficiently Protected Credentials vulnerability. This could allow an attacker to retrieve pins including the Master Pin, overriding standard user permissions.	8.1	More Details
	VoltAgent through 2.1.20 fails to validate conversation ownership in memory API handlers, allowing		

CVE-2026-82283	authenticated users to access other users' conversations. Attackers can read, modify, and delete arbitrary conversations and messages by supplying caller-controlled identifiers to memory endpoints.	8.1	More Details
CVE-2026-53580	Trilium is an open-source hierarchical note-taking application. In versions prior to 0.104.0, the automatic image-download feature accepts file:// URLs in a note's img tags and reads the referenced local file with no path validation, allowing any authenticated user to disclose arbitrary files readable by the Trilium process. When a text note is saved, Trilium scans its HTML for image sources and downloads each external one; because the HTML sanitizer keeps file as an allowed scheme, a source such as file:///etc/passwd is passed straight to a filesystem read and its contents are stored as a note attachment the user can then retrieve. Pointing the same primitive at an unbounded source such as /dev/zero causes uncontrolled memory allocation that crashes the server process. The feature is enabled by default and is reachable through the web UI, the ETAPI, the web clipper, and note imports, requiring only an authenticated session or an ETAPI token. This issue is fixed in version 0.104.0	8.1	More Details
CVE-2026-82291	HeyForm before 3.0.0-rc.8 reflects the request Origin header in CORS responses while allowing credentials, enabling cross-origin requests with authentication. Attackers can execute authenticated GraphQL queries from malicious pages visited by logged-in users to access workspaces, projects, forms, submissions, and respondent data, or modify account settings.	8.1	More Details
CVE-2026-82279	HyperDX through 1.10.1 fails to enforce role-based access controls in team management endpoints, allowing any team member to perform administrative actions. Attackers can delete team members including owners, rotate API keys, and rename teams by sending requests to PATCH /team/apiKey, PATCH /team/name, and DELETE /team/member endpoints.	8.1	More Details
CVE-2026-81522	A weakness in the MongoDB C++ Driver's handling of caller-supplied namespace identifiers allows special characters embedded in those identifiers. An application that builds a namespace identifier from untrusted input without validating it may therefore have its operation directed at a different target than intended. This can result in limited unauthorized read and write access to data belonging to another logical tenant of the affected application.	8.1	More Details
CVE-2026-54083	Wazuh is an open-source security platform providing unified XDR and SIEM protection for endpoints and cloud workloads. The ip-customblock active response script contains a path traversal vulnerability that lets an attacker create or delete arbitrary files on the filesystem as root. The script builds a file path by concatenating the srcip field taken from alert JSON directly onto the fixed /ipblock/ base directory, without validating that the value is a well-formed IP address. Because the extraction routine returns the raw string unchecked, an attacker who can trigger alert-matching log events with a crafted srcip containing ../ sequences can escape the base directory. The block action opens the resulting path in append mode, creating an empty file at an arbitrary location, while the unblock action passes it to remove(), deleting an arbitrary file; since the active response daemon runs as root, this includes sensitive files such as system credentials and Wazuh configuration. Unlike the sibling scripts host-deny.c, default-firewall-drop.c, and firewalld-drop.c, which reject non-IP input via get_ip_version(), ip-customblock.c omits this validation. This issue is fixed in version 4.14.7.	8.1	More Details
CVE-2026-81525	The MongoDB client library for PHP does not sufficiently sanitize special elements in application-supplied namespace identifiers before using them to construct the target namespace for database operations. An application that incorporates untrusted text into these identifiers may have operations silently directed at a different storage location than the one the application intended.	8.1	More Details
CVE-2026-81728	Dolibarr before 24.0.0 contains a SQL injection in its CSV and XLSX import wizard. The wizard reads its update keys with GETPOST('updatekeys', 'array') in htdocs/imports/import.php, which applies only the generic alphanohtml filter: that strips HTML but leaves SQL keywords, comment markers, parentheses, spaces and quotes intact. import_insert() in htdocs/core/modules/import/import_csv.modules.php then iterates the submitted values and builds a filter with $where[] = $key.' = '.$data[$key], having first applied preg_replace('/^.*\./i', '', $key), an alias strip that does nothing to a value containing no dot. The assembled string is executed through $this->db->query(). The injected SELECT resolves the row id that the import then assigns to $lastinsertid, which becomes the WHERE target of a subsequent UPDATE, so a UNION SELECT returning an attacker-chosen integer both exfiltrates arbitrary table content and redirects which row the import overwrites; for category link tables the raw filter array is spliced into that UPDATE directly. The interface offers a fixed list of legitimate column codes but the server never checks the submitted values against it. A user holding the import permission can exploit this. Release 23.0.4 does not carry the fix; the allow-list test was added in 24.0.0.	8.1	More Details
CVE-2026-15985	The Classified Listing - Mobile Number Verification plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 1.6.0. This is due to missing server-side Firebase OTP validation in the process_otp_login() function. This makes it possible for unauthenticated attackers to authenticate as any user with a phone number registered in the plugin's phone table by submitting an arbitrary OTP code and UID through the Firebase OTP login flow. Successful exploitation requires OTP login to be enabled with Firebase selected as the verification gateway, and requires the attacker to know or guess the target account's registered phone number. Administrator account takeover is possible if an administrator account has a phone number registered in the plugin.	8.1	More Details
CVE-2026-82269	Gophish through 0.12.1 fails to enforce account lockout and password change requirements in the API authentication middleware. Attackers with valid API keys can bypass these security controls and retain full	8.1	More Details

	API access even when their account is locked or password change is required.		
CVE-2026-50979	A command injection vulnerability in the 'advanced/curl' component of Osbil Technology oPanel v1.19.50 and earlier allows authenticated attackers to execute arbitrary shell commands via the 'url' parameter	8.1	More Details
CVE-2026-43621	Simple Machines Forum (SMF) through 2.1.7, fixed in commit 6f0dc61, contains an authorization state-confusion vulnerability in the profile loader that allows authenticated low-privileged users to gain administrator access by supplying multiple values for the user parameter. Attackers can exploit the mismatch between Profile::$member and User::$me->is_owner during sequential profile loading to be treated as the owner of an administrator profile, enabling unauthorized password changes and full account takeover.	8.1	More Details
CVE-2026-82287	Rybbit before 2.7.0 contains a CORS misconfiguration vulnerability that allows attackers to bypass origin restrictions by reflecting any request origin in Access-Control-Allow-Origin responses while credentials are enabled. Attackers can issue credentialed cross-origin requests from any website to read analytics data, account information, and perform authenticated state-changing operations as the victim user.	8.1	More Details
CVE-2026-66047	ProfilePress (wp-user-avatar) WordPress plugin before 4.17.2 contains an unauthenticated remote code execution vulnerability that allows unauthenticated attackers to install and activate arbitrary plugins by brute-forcing a weak 32-bit connect token via the ppress_connect_process AJAX handler. Attackers can supply a caller-controlled URL through the file request parameter to trigger silent plugin installation and activation, achieving PHP code execution as the web-server user.	8.1	More Details
CVE-2026-77317	SeaweedFS is a distributed storage system for files and blobs. In versions from 3.88 through 4.39, the SFTP server evaluates configured path permissions with a literal string-prefix comparison, so a user scoped to a path is also granted the same access to any sibling path whose name merely begins with the same characters. A user granted access to /tenants/alice therefore also matches /tenants/alice-archive, /tenants/alice2, and similar siblings, because the check does not require a path-component boundary. An authenticated low-privilege SFTP user with a root home directory and narrow path permissions can thereby cross the configured ACL boundary to read another tenant's files, and to overwrite them if granted write, all through the documented SFTP service with its own valid credentials. This issue is fixed in version 4.40.	8.1	More Details
CVE-2026-80599	In the Linux kernel, the following vulnerability has been resolved: batman-adv: dat: ensure accessible eth_hdr proto field When batadv_get_vid() accesses the proto field of the ethernet header, it is not checking if the data itself is accessible. The caller is responsible for it. But in contrast to other call sites, batadv_dat_get_vid() and its caller didn't make sure this is true. This could have caused an out-of-bounds access.	8.1	More Details
CVE-2026-19423	The Ultimate Member WordPress plugin before 2.13.0 does not validate a submitted role selection when it cannot resolve the set of roles a profile form permits, and screens the value against the site's registered role names rather than against the form's own allow-list, allowing unauthenticated users who register through the Ultimate Member WordPress plugin before 2.13.0's own form to grant themselves arbitrary capabilities and reach administrator-equivalent access.	8.1	More Details
CVE-2026-81273	Unauthenticated Cross Site Request Forgery (CSRF) in FluentBooking Pro <= 2.2.4 versions.	8.1	More Details
CVE-2026-82282	Atlantis through 0.47.1 fails to authenticate the /github-app/setup endpoint, allowing unauthenticated attackers to access GitHub App credentials. Attackers can observe or intercept the GitHub redirect during setup to obtain the RSA private key and webhook secret, enabling installation token minting and webhook payload forgery.	8.0	More Details
CVE-2026-59307	An operator who calls JdbcMessageStore.addAllowedPatterns(...) to restrict deserialization receives no protection at all when the store is a Spring-managed bean. Spring Integration 7.1.0 Spring Integration 7.0.0 - 7.0.5 Spring Integration 6.5.0 - 6.5.10 Spring Integration 6.4.0 - 6.4.12	8.0	More Details
CVE-2026-77586	In MongoDB Connector for BI, MongoDB object names such as collection, field, and index names are placed into the quoted identifiers of the DDL text returned by SHOW CREATE statements without escaping the identifier delimiter. A user with permission to write to a sampled MongoDB collection can choose a name that closes the quoted identifier early, so that additional SQL text becomes part of the generated output. If an operator or automated tool later replays that generated statement against a SQL server, the additional text is executed with the privileges of that session.	8.0	More Details
CVE-2026-75486	Synk Sweater Comb before 3.8.8 contains a command injection vulnerability that allows an attacker who controls the .vervet.yaml configuration file to execute arbitrary OS commands by injecting malicious input into the linters.<key>.optic-ci.original branch name field. The expectGitBranch() function in src/lint.ts passes the unsanitized branch name directly into child_process.exec() via an unescaped template literal, enabling arbitrary command execution when the lint command is run against the repository.	8.0	More Details
CVE-2026-80550	In the Linux kernel, the following vulnerability has been resolved: s390/vfio_ccw: Fix out of bounds check on CCW array The routine ccwchain_calc_length() counts the number of channel command words (CCWs) that are chained together in a single channel program, and rejects anything larger than CCWCHAIN_LEN_MAX (256) CCWs. The loop itself is "do..while (count < 257)", and while the logic in is_cpa_within_range() correctly adjusts between the 0-index array of CCWs and the count of CCWs starting at 1, this means it would look at a possible 257th CCW before ending the loop and (correctly) returning an error. Fix this by	7.9	More Details

	restructuring the loop to break as soon as 256 CCWs (thus indexes 0-255) are examined, without looking at memory outside the range.		
CVE-2026-82636	Qubes OS before qubes-core-dom0-linux 4.3.22 allows OS command injection during a qvm-copy-to-vm call from dom0 to an attacker-controlled qube, because the "system" library function is used to process an error message that may have shell metacharacters. This occurs in core-admin-linux/file-copy-vm/qfile-dom0-agent.c.	7.9	More Details
CVE-2026-44629	Improper access control to the Synergis Softwire installation folder. This vulnerability affects Streamvault all-in-one appliances (SV-100E and SV-300E series) and Synergis Softwire installed on Windows servers.	7.9	More Details
CVE-2026-80606	In the Linux kernel, the following vulnerability has been resolved: drm/xe/userptr: Hold notifier_lock for write on inject test path When CONFIG_DRM_XE_USERPTR_INVAL_INJECT=y, xe_pt_svm_userptr_pre_commit() runs vma_check_userptr() with the svm notifier_lock taken for read. The test injection causes vma_check_userptr() to call xe_vma_userptr_force_invalidate(), which feeds into xe_vma_userptr_do_inval() with drm_gpusvm_ctx.in_notifier=true. That flag tells drm_gpusvm_unmap_pages() the caller already holds notifier_lock for write and only asserts the mode. Because the caller actually holds it for read, the assertion fires: WARNING: drivers/gpu/drm/drm_gpusvm.c:1669 at \ drm_gpusvm_unmap_pages+0xd4/0x130 [drm_gpusvm_helper] Call Trace: xe_vma_userptr_do_inval+0x40d/0xfd0 [xe] xe_vma_userptr_invalidate_pass1+0x3e6/0x8d0 [xe] xe_vma_userptr_force_invalidate+0xde/0x290 [xe] vma_check_userptr.constprop.0+0x1c6/0x220 [xe] xe_pt_svm_userptr_pre_commit+0x6a3/0xc60 [xe] ... xe_vm_bind_ioctl+0x3a0a/0x4480 [xe] Acquire notifier_lock for write in pre-commit when the inject Kconfig is enabled, via new helpers xe_pt_svm_userptr_notifier_lock()/_unlock(). Rename xe_svm_assert_held_read() to xe_svm_assert_held_read_or_inject_write() so it asserts the correct mode under each build configuration. Production builds (CONFIG_DRM_XE_USERPTR_INVAL_INJECT=n) keep the existing read-mode behavior bit-for-bit. (cherry picked from commit 80ccbd97ffee8ad2e73167d826fe7be548364365)	7.8	More Details
CVE-2026-80613	In the Linux kernel, the following vulnerability has been resolved: veth: fix NAPI leak in XDP enable error path During XDP enablement in veth, if xdp_rxq_info_reg() or xdp_rxq_info_reg_mem_model() fails, the driver rolls back the changes. However, the rollback loop: for (i--; i >= start; i--) { decrements the loop index 'i' before the first iteration. This correctly skips unregistering the rxq for the failed index 'i' (as registration failed or was already cleaned up), but it also erroneously skips calling netif_napi_deli() for rq[i].xdp_napi. Since netif_napi_add() was already called for index 'i', this leaves a dangling napi_struct in the device's napi_list. When the veth device is later destroyed, the freed queue memory (which contains the leaked NAPI structure) can be reused. The subsequent device teardown iterates the NAPI list and corrupts the reallocated memory, leading to UAF. Fix this by explicitly deleting the NAPI association for the failed index 'i' before rolling back the successfully configured queues.	7.8	More Details
CVE-2026-81572	In CodeMeter Runtime from version 8.40 to (excluding) 8.41a and 9.00 to (excluding) 9.10, cmu.exe --create-io --file C: creates a predictable temporary file under C:\CM-Stick. The directory and file paths are not properly checked for NTFS reparse points, such as junctions or symbolic links, before file operations are performed. A local attacker can create a junction at the temporary file that points to an arbitrary system path. Because CodeMeter Runtime runs with System privileges, this could allow arbitrary files to be deleted with System privileges and potentially enable local privilege escalation.	7.8	More Details
CVE-2026-80598	In the Linux kernel, the following vulnerability has been resolved: ntfs3: fix out-of-bounds read in decompress_lznt decompress_lznt() does not validate array index bounds before accessing the decompression table. A corrupted NTFS3 image with invalid compressed data can trigger an out-of-bounds read. Add index bounds checking to prevent the OOB access.	7.8	More Details
CVE-2026-80619	In the Linux kernel, the following vulnerability has been resolved: apparmor: fix potential UAF in aa_replace_profiles The function aa_replace_profiles was accessing udata->size after calling aa_put_loaddata(udata), causing a potential UAF. Fixed this by saving the size to a local variable before dropping the reference.	7.8	More Details
CVE-2026-80661	In the Linux kernel, the following vulnerability has been resolved: ufs: core: tracing: Do not dereference pointers in TP_printk() The trace events in drivers/ufs/core/ufs_trace.h were converted to take a pointer to the hba structure as an argument for the tracepoint and then in TP_printk() the printing of the dev_name from the ring buffer was converted to using the dev dereferenced pointer from the hba saved pointer. This is not allowed as the TP_printk() is executed at the time the trace event is read from /sys/kernel/tracing/trace file. That can happen literally, seconds, minutes, hours, weeks, days, or even months later! There is no guarantee that the hba pointer will still exist by the time it is dereferenced when the "trace" file is read. Instead, save the device name from the hba pointer at the time the tracepoint is called and place it into the ring buffer event. Then the TP_printk() can read the name directly from the ring buffer and remove the possibility that it will read a freed pointer and crash the kernel. This was detected when testing the trace event code that looks for TP_printk() parameters doing illegal derferences[1] [1] https://lore.kernel.org/all/20260630184836.74d477b6@gandalf.local.home/	7.8	More Details
CVE-2026-	In the Linux kernel, the following vulnerability has been resolved: char: tlclk: fix use-after-free in tlclk_cleanup() This patch improves the module cleanup process in the tlclk driver to prevent potential use-after-free and race conditions. Currently, the file_operations structure does not specify the .owner field, which could allow the module to be unloaded while user-space processes are still interacting with the device. Additionally, the tlclk_cleanup() function frees the alarm_events memory before ensuring that	7.8	More

80622	blocked processes in the waitqueue are fully awakened and that the switchover_timer has completed. To address these cases, this patch: - Sets '.owner = THIS_MODULE' in tlclk_fops to safely defer module unloading while the device is in use. - Updates tlclk_cleanup() to explicitly wake up all blocked readers (wake_up_all), properly release hardware I/O regions, and safely delete the timer (timer_delete_sync) prior to freeing memory.		Details
CVE-2026-80628	In the Linux kernel, the following vulnerability has been resolved: ALSA: seq: oss: Serialize readq reset state with q->lock snd_seq_oss_readq_clear() resets qlen, head, and tail without q->lock even though the normal reader and producer paths serialize the same ring state under that spinlock. A reset can therefore race snd_seq_oss_readq_free() or snd_seq_oss_readq_put_event() and leave stale records in the queue, drop freshly queued ones, or report the wrong readiness after wakeup. KCSAN reports a data race between snd_seq_oss_readq_clear() and snd_seq_oss_readq_free(). Take q->lock while clearing the ring and resetting input_time. Factor the enqueue logic into a caller-locked helper so snd_seq_oss_readq_put_timestamp() updates its suppression state under the same lock instead of racing the reset path. The buggy scenario involves two paths, with each column showing the order within that path: reset path: locked readq updater: 1. snd_seq_oss_reset() or 1. A reader or callback producer release reaches takes q->lock on the same queue. snd_seq_oss_readq_clear(). 2. snd_seq_oss_readq_clear() 2. The updater tests or modifies resets qlen, head, tail, qlen, head, and tail. and input_time. 3. snd_seq_oss_readq_clear() 3. The updater completes its wakes sleepers on read-modify-write sequence. q->midi_sleep. 4. Without q->lock, the reset 4. The resulting ring state drives can overlap the locked later reads and readiness. update. KCSAN reports: BUG: KCSAN: data-race in snd_seq_oss_readq_clear / snd_seq_oss_readq_free write to 0xffff8881069fe608 of 4 bytes by task 120516 on cpu 0: snd_seq_oss_readq_free+0x6c/0x80 snd_seq_oss_read+0xcb/0x250 odev_read+0x38/0x60 vfs_read+0xff/0x600 ksys_read+0xb4/0x140 __x64_sys_read+0x46/0x60 do_syscall_64+0xbb/0x2f0 entry_SYSCALL_64_after_hwframe+0x77/0x7f read to 0xffff8881069fe608 of 4 bytes by task 120517 on cpu 1: snd_seq_oss_readq_clear+0x1f/0x90 snd_seq_oss_reset+0xa7/0xf0 snd_seq_oss_ioctl+0x6f6/0x7e0 odev_ioctl+0x56/0xc0 __x64_sys_ioctl+0xd1/0x120 do_syscall_64+0xbb/0x2f0 entry_SYSCALL_64_after_hwframe+0x77/0x7f value changed: 0x00000001 -> 0x00000000	7.8	More Details
CVE-2026-80591	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix listxattr handling of corrupted xattr entries Validate the xattr entry before reading its fields in f2fs_listxattr(). Return -EFSCORRUPTED when the entry is outside the valid xattr storage area instead of returning a successful partial result.	7.8	More Details
CVE-2026-77652	A heap-based buffer overflow vulnerability exists in the Dia diagram editor WPG file format importer. In plug-ins/wpg/wpg-import.c, the WPG import renderer allocates a fixed palette with: ren->pPal = g_new0(WPGColorRGB, 256); When handling a WPG_COLORMAP record, the parser reads a start index (i16) and number of colors (iNum16) from the file and reads palette data with: bRet &= (iNum16 == (int)fread(&ren->pPal[i16], sizeof(WPGColorRGB), iNum16, f)); The only bounds-related check is `if (i16 >= 0 && i16 <= iSize)`, where iSize is the WPG record size—not the palette capacity. There is no validation that i16 is less than 256 or that i16 + iNum16 does not exceed 256. A malicious WPG file can supply i16=256 and iNum16=264. That causes fread() to write 792 bytes starting at &pPal[256], while the palette buffer is only 768 bytes (256 entries × 3 bytes). This overflows into adjacent heap metadata and can crash Dia (SIGABRT / malloc corruption errors) or, depending on heap layout and exploit primitives, potentially lead to arbitrary code execution. Exploitation requires convincing a user to open a crafted WPG file via Dia's file dialog, command line, or file association. No special privileges are required to deliver the file to the victim. Affected component: WPG parser (plug-ins/wpg/wpg-import.c). Affected versions: all Dia versions containing this code path (reporter tested Dia 0.98+git20260221-1; issue present on upstream master as of 2026-08-21).	7.8	More Details
CVE-2026-80649	In the Linux kernel, the following vulnerability has been resolved: firmware: arm_scmi: Fix OOB in scmi_power_name_get() scmi_power_name_get() does not validate the domain number passed by the external caller, which may lead to an out-of-bounds access. Fix this by returning "unknown" for invalid domains, like scmi_reset_name_get() does.	7.8	More Details
CVE-2026-80656	In the Linux kernel, the following vulnerability has been resolved: hfsplus: Add a sanity check for btree node size Syzbot reported an uninit-value bug in [1] with a corrupted HFS+ image, during the file system mounting process, specifically while loading the catalog, a corrupted node_size value of 1 caused the rec_off argument passed to hfs_bnode_read_u16() (within hfs_bnode_find()) to be excessively large. Consequently, the function failed to return a valid value to initialize the off variable, triggering the bug [1]. Every node starts from BTree node descriptor: struct hfs_bnode_desc. So, the size of node cannot be lesser than that. However, technical specification declares that: "The node size (which is expressed in bytes) must be power of two, from 512 through 32,768, inclusive." Add a check for btree node size base on technical specification. [1] BUG: KMSAN: uninit-value in hfsplus_bnode_find+0x141c/0x1600 fs/hfsplus/bnode.c:584 hfsplus_bnode_find+0x141c/0x1600 fs/hfsplus/bnode.c:584 hfsplus_btree_open+0x169a/0x1e40 fs/hfsplus/btree.c:382 hfsplus_fill_super+0x111f/0x2770 fs/hfsplus/super.c:553 get_tree_bdev_flags+0x6e6/0x920 fs/super.c:1694 get_tree_bdev+0x38/0x50 fs/super.c:1717 hfsplus_get_tree+0x35/0x40 fs/hfsplus/super.c:709 vfs_get_tree+0xb3/0x5d0 fs/super.c:1754 fc_mount fs/namespace.c:1193 [inline]	7.8	More Details
CVE-2026-80526	In the Linux kernel, the following vulnerability has been resolved: ASoC: tas2562: Validate values for volume writes tas2562_volume_control_put() does not do any validation of the control value written by userspace, it uses it to look up a value in a fixed size array which can easily be overflowed and then writes whatever value it gets back to the device. Add validation that we are loading a value we have in the array.	7.8	More Details

CVE-2026-80682	In the Linux kernel, the following vulnerability has been resolved: riscv/mm: use physical alignment for vmemmap_start_pfn RISC-V computes vmemmap_start_pfn by rounding phys_ram_base down to VMEMMAP_ADDR_ALIGN. That alignment must therefore be expressed in the physical-address domain. Commit 476849b0fba4 ("riscv/mm: align vmemmap to maximal folio size") attempted to account for the maximal folio alignment by feeding MAX_FOLIO_VMEMMAP_ALIGN directly into VMEMMAP_ADDR_ALIGN. However, MAX_FOLIO_VMEMMAP_ALIGN is measured in bytes of struct page storage, whereas VMEMMAP_ADDR_ALIGN is used to align a physical address. The mask-based compound_info encoding requires pfn_to_page(0) to be naturally aligned to MAX_FOLIO_VMEMMAP_ALIGN. Commit 9f94db4c7eaa ("mm/sparse: check memmap alignment for compound_info_has_mask()") added a check for that requirement and exposed the unit mismatch on systems such as QEMU virt, where the DRAM base is not aligned to MAX_FOLIO_NR_PAGES * PAGE_SIZE. Here is the log: [0.000000][C0] ------------[cut here]------------ [0.000000][C0] WARNING: mm/sparse.c:365 at sparse_init+0x58a/0x6fe, CPU#0: swapper/0 [0.000000][C0] Modules linked in: [0.000000][C0] CPU: 0 UID: 0 PID: 0 Comm: swapper Not tainted 7.2.0-rc3-g1d8304bdd65f #2 PREEMPT [0.000000][C0] Hardware name: riscv-virtio,qemu (DT) [0.000000][C0] epc : sparse_init+0x58a/0x6fe [0.000000][C0] ra : sparse_init+0x58a/0x6fe [0.000000][C0] epc : ffffffff86851c88 ra : ffffffff86851c88 sp : ffffffff88807a30 [0.000000][C0] gp : ffffffff8a3bf240 tp : ffffffff88842080 t0 : ff600000ffab6000 [0.000000][C0] t1 : 000000017fab6000 t2 : 65203a6573726363 s0 : ffffffff88807bc0 [0.000000][C0] s1 : 000000000e000000 a0 : 0000000000000007 a1 : 0000000000000000 [0.000000][C0] a2 : 0000000000000002 a3 : ffffffff86851c88 a4 : 0000000000000000 [0.000000][C0] a5 : ffffffff88843080 a6 : 0000000000000003 a7 : 0000000000000000 [0.000000][C0] s2 : ff600000000000000 s3 : 0040000000000000 s4 : 0004000000000000 [0.000000][C0] s5 : ffffffff8a4d92e0 s6 : ff600000ffab55e0 s7 : ffffffff88384d00 [0.000000][C0] s8 : 0000000000000003 s9 : ffffffff88384cc1 s10: ffffffff88384cc0 [0.000000][C0] s11: ffffffff8a4daae0 t3 : ffffffff915e8b20 t4 : ffffffff915e8b20 [0.000000][C0] t5 : ffffffff915e8b20 t6 : ffffffff915e8bc8 ssp : 0000000000000000 [0.000000][C0] status: 0000000200000100 badaddr: ffffffff86851c88 cause: 0000000000000003 [0.000000][C0] [<ffffffff86851c88>] sparse_init+0x58a/0x6fe [0.000000][C0] [<ffffffff8683d396>] mm_core_init_early+0x116/0x1e30 [0.000000][C0] [<ffffffff86801edc>] start_kernel+0xd2/0x848 Convert MAX_FOLIO_VMEMMAP_ALIGN to the equivalent physical alignment before using it in VMEMMAP_ADDR_ALIGN. This keeps the existing round_down() logic while making the resulting vmemmap base satisfy the mask-alignment requirement.	7.8	More Details
CVE-2026-80531	In the Linux kernel, the following vulnerability has been resolved: xfs: avoid UAF on sc->tempip in xrep_tempfile_create LOLLM noticed a potential UAF if the tempfile creation code fails after it set sc->tempip. Fix that.	7.8	More Details
CVE-2026-80521	In the Linux kernel, the following vulnerability has been resolved: af_unix: Unlink scc_entry in unix_del_edge(). Kyle Zeng reported that GC could free a dead SCC partially. The scenario is as follows: 1) Create two SCCs: X -. A <-> B ^--' 2) Run the following concurrently: 2-1) send() sk-B to sk-B from sk-X 2-2) close() both A and B At 2-1), there is a small window where unix_add_edges() publishes a new edge (B <-> B) to GC but its skb is not queued by skb_queue_tail(). If 2-2) completes before skb_queue_tail() and GC is triggered, it judges A <-> B as dead, but B is not freed because GC cannot collect the not-yet-queued skb holding the B <-> B edge. X -. A <-> B -. This edge is visible ^--' ^..' but skb is not This itself is not a problem since the next GC run will judge B as dead as well and free it finally. X -. A <.> B -. ^--' ^--' However, X's SCC forces the next GC to call unix_walk_scc_fast(), and it iterates over A through B's scc_entry. Let's unlink scc_entry before freeing the vertex in unix_del_edge().	7.8	More Details
CVE-2026-80677	In the Linux kernel, the following vulnerability has been resolved: driver core: use READ_ONCE() for dev->driver in dev_has_sync_state() dev_has_sync_state() reads dev->driver twice without holding device_lock() -- once for the NULL check and once to dereference ->sync_state. Some callers only hold device_links_write_lock, which doesn't prevent a concurrent unbind from clearing dev->driver via device_unbind_cleanup(). Fix it by reading dev->driver exactly once with READ_ONCE(), pairing with the WRITE_ONCE() in device_set_driver().	7.8	More Details
CVE-2026-74753	In the Linux kernel, the following vulnerability has been resolved: perf: Reject exited events as group leaders perf_event_remove_on_exec() sets remove-on-exec events to the EXIT state and detaches their group relationships. The event's file descriptor can remain open, however, and perf_event_open() currently accepts that event as a group leader because its early validation rejects only REVOKED and DEAD events. A new sibling can consequently be linked to the detached leader. When the leader is closed, perf_group_detach() observes that its PERF_ATTACH_GROUP bit is already clear and skips the new sibling. The sibling then retains a group_leader pointer to the freed event. Reject group leaders in the EXIT state. Perform the check while holding the shared context mutex so that an exec in the target task cannot detach the leader between validation and group attachment. [peterz: make the earlier test fully consistent]	7.8	More Details
CVE-2026-74748	In the Linux kernel, the following vulnerability has been resolved: netfilter: ipset: fix refcount race between list:set GC and swap __ip_set_put_byindex() resolved the index to a set pointer under RCU, then took ip_set_ref_lock in __ip_set_put() to decrement set->ref. ip_set_swap() holds that same lock while swapping both the ip_set_list slots and the two sets' ref counters, so it can interleave between the dereference and the lock acquisition, leaving the caller to decrement a set whose reference already moved to the other index and hit BUG_ON(set->ref == 0). list_set_gc() reaches this from timer softirq, which the nfnl mutex does not serialize against swap: an expiring list:set member calls list_set_del() -> ip_set_put_byindex() while IPSET_CMD_SWAP runs on the referenced sets. Resolve the index and decrement under ip_set_ref_lock, as	7.8	More Details

	ip_set_swap() already does, keeping the refcount tied to the index rather than to a stale set pointer. kernel BUG at net/netfilter/ipset/ip_set_core.c:685! Oops: invalid opcode: 0000 [#1] SMP KASAN NOPTI RIP: 0010:ip_set_put_byindex (net/netfilter/ipset/ip_set_core.c:870) Call Trace: <IRQ> list_set_del (net/netfilter/ipset/ip_set_list_set.c:159) set_cleanup_entries (net/netfilter/ipset/ip_set_list_set.c:181) list_set_gc (net/netfilter/ipset/ip_set_list_set.c:578) call_timer_fn (kernel/time/timer.c:1748) __run_timers (kernel/time/timer.c:1799 kernel/time/timer.c:2374) run_timer_softirq (kernel/time/timer.c:2405) </IRQ> Kernel panic - not syncing: Fatal exception in interrupt		
CVE-2026-74747	In the Linux kernel, the following vulnerability has been resolved: ipvs: revalidate ihl to prevent out-of-bounds access While the outer IP header is already pulled into the skb head, we must be careful and revalidate the embedded headers after reading them from the skb frags to prevent out-of-bounds access. One such place reported by Sashiko is ip_vs_nat_icmp() where local process can change the ihl field and after skb_ensure_writable() we can see larger value which is a problem for the ip_send_check(cih) calls. Add check to drop the packet if the ihl field is changed.	7.8	More Details
CVE-2026-74739	In the Linux kernel, the following vulnerability has been resolved: net/sched: cls_u32: skip hash tables in u32_bind_class() u32_walk() enumerates both struct tc_u_hnode and struct tc_u_knode through the walker callback. u32_bind_class() unconditionally casts the passed fh to tc_u_knode and accesses &n->res, so when fh is actually a tc_u_hnode, which has no tcf_result member, this results in a slab-out-of-bounds read of res->classid in tc_cls_bind_class(). The issue can be reproduced with the following commands: tc qdisc add dev lo root handle 1: hfsc tc class add dev lo parent 1: classid 1:1 hfsc sc rate 1000kbit tc filter add dev lo parent 1:1 protocol ip prio 1 u32 match u32 0 0 flowid 1:1 tc class add dev lo parent 1: classid 1:2 hfsc sc rate 2000kbit Fix this by skipping hash tables via the TC_U32_KEY(handle) check.	7.8	More Details
CVE-2026-74736	In the Linux kernel, the following vulnerability has been resolved: net/sched: cls_bpf: reject dev-bound programs bound to a different device cls_bpf_prog_from_efd() obtained a SCHED_CLS program via bpf_prog_get_type_dev() but never verified that a device-bound (offloaded) program's bound netdev matches the TC netdev the classifier is being attached to. This let a program loaded with prog_ifindex for device A be attached via cls_bpf + skip_sw to device B; deleting device A then destroyed the program's offload state while it was still attached to device B, triggering a netdevsim WARN (panic with panic_on_warn=1). Mirror the XDP attach path (net/core/dev.c) and reject the attach with -EINVAL when a dev-bound program's bound device does not match the target device.	7.8	More Details
CVE-2026-80680	In the Linux kernel, the following vulnerability has been resolved: i2c: amd-mp2: Unregister callback on adapter add failure amd_mp2_register_cb() stores the platform I2C context in the MP2 PCI driver's callback table before the adapter is registered. If i2c_add_adapter() fails, probe returns and devres frees the context, but the PCI driver can still dereference the stale pointer from its IRQ and system-sleep callbacks. Unregister the callback before returning the adapter registration error.	7.8	More Details
CVE-2026-77658	A stack-based buffer overflow vulnerability exists in the Dia diagram editor when processing Network Bus objects from Dia XML project files. In objects/network/bus.c, bus_load() reads the number of bus handles from the file attribute "bus_handles" using attribute_num_data() without validating an upper bound: bus->num_handles = attribute_num_data(attr); When a bus handle is subsequently moved, bus_handle_moved() allocates two temporary arrays on the stack: parallel = (real *)g_alloca(num_handles * sizeof(real)); perp = (real *)g_alloca(num_handles * sizeof(real)); Because num_handles is fully attacker-controlled via the project file, sufficiently large values (for example 262144 or higher) cause g_alloca() to consume more stack space than the default thread stack limit (typically 8 MB on Linux), resulting in stack overflow, SIGSEGV, and potential stack frame / return-address corruption. An attacker can embed a Bus object with an excessive bus_handles count in a malicious .dia file. Exploitation requires the victim to open the file in Dia (file dialog, command line, or file association) and trigger handle manipulation (moving a bus handle), which exercises the vulnerable code path. The identical g_alloca pattern is present in objects/Misc/tree.c (copied from bus.c) and is likely vulnerable to the same class of attack via Tree objects. Affected versions: Dia 0.98.0 and earlier versions containing this code; issue confirmed on upstream master as of 2026-08-21. Upstream report: https://gitlab.gnome.org/GNOME/dia/-/issues/581	7.8	More Details
CVE-2026-80718	In the Linux kernel, the following vulnerability has been resolved: mm/percpu-km: fix bitmap overflow and accounting in pcpu_create_chunk() In pcpu_create_chunk(), nr_pages is the total contiguous backing allocation, i.e., nr_units * pcpu_unit_pages, but pcpu_chunk_populated() uses it to set chunk->populated, whose size is pcpu_unit_pages, bitmap. Since bit N in chunk->populated means page offset N inside every unit is backed. When nr_units > 1, the function writes beyond chunk->populated. Fix it by using chunk->nr_pages. It also fixes the global pcpu_nr_empty_pop_pages accounting, since pcpu_balance_free() only iterates up to chunk->nr_pages. Commit a63d4ac4ab609 ("percpu: make percpu-km set chunk->populated bitmap properly") introduced the bitmap overflow issue. Later, commit b539b87fed37f ("percpu: implmeent pcpu_nr_empty_pop_pages and chunk->nr_populated") added pcpu_nr_empty_pop_pages and caused the accounting issue.	7.8	More Details
CVE-2026-81719	openssl_encrypt before 1.4.9 executes untrusted third-party plugins with insufficient controls: the plugin signature policy defaulted to WARN, so an unsigned/unverifiable non-built-in plugin was compiled and executed in the host process at import time, before the runtime sandbox is installed. The only default gate was an incomplete, bypassable AST denylist. If a user is induced to load an attacker's plugin, this results in arbitrary code execution with the privileges of the user running openssl_encrypt. Fixed in 1.4.9 by defaulting the signature policy to ENFORCE for non-built-in plugins.	7.8	More Details
	In the Linux kernel, the following vulnerability has been resolved: ASoC: codecs: lpass-tx-macro: Fix enum		

CVE-2026-80583	kcontrol accesses The "DEC0 MODE" to "DEC7 MODE" controls are enumerated, but tx_macro_dec_mode_get() and tx_macro_dec_mode_put() access their value through ucontrol->value.integer.value[0] (a long) instead of ucontrol->value.enumerated.item[0] (an unsigned int). This same pattern was fixed in the sibling drivers by commit bcfe5f76cc40 ("ASoC: codecs: rx-macro: fix accessing array out of bounds for enum type") and commit 0ea5eff7c606 ("ASoC: codecs: va-macro: fix accessing array out of bounds for enum type"), but tx-macro was missed. On 64-bit kernels built with CONFIG_SND_CTL_DEBUG, the elem value sanity check catches the 4 bytes written past the enumerated item and every read of these controls fails with -EINVAL: snd-sm8250 sound: control 2:0:0:DEC0 MODE:0: access overflow	7.8	More Details
CVE-2026-80716	In the Linux kernel, the following vulnerability has been resolved: ALSA: pcm: wake linked drain waiters on unlink snd_pcm_drain() on a linked stream parks an on-stack wait entry on the drained peer's runtime->sleep, and after schedule_timeout() removes it only if that peer is still found in the caller's group. If group membership changes during the wait and the sleep ends by signal or timeout (so autoremove_wake_function() does not run), finish_wait() is skipped and snd_pcm_drain() returns with the entry still queued on that stream's sleep list; a later wake_up() then walks a freed stack frame. This is reachable by unlinking either the drained or the draining stream. Unlike the close path (snd_pcm_drop() -> snd_pcm_post_stop()), snd_pcm_unlink() never wakes the sleep queues. Wake every group member under the group lock before the membership change, so a linked drainer is released and drops its entry while the streams are still grouped. The window was opened when snd_pcm_link_rwsem stopped being held across the wait and the removal became conditional on group membership (see Fixes). The later switch to finish_wait() kept that conditional removal, so the signal/timeout case remained.	7.8	More Details
CVE-2026-80696	In the Linux kernel, the following vulnerability has been resolved: hwmon: (ltc4282) Fix reading the minimum alarm voltage Coverity reports an out-of-bounds access when reading the minimum alarm voltage for the VGPIO channel. Add the missing return statement to fix the problem.	7.8	More Details
CVE-2026-58094	The FIOSSHMLPGCNF ioctl(2) operation configures the page size for a largepage shared memory object. This is intended to be used immediately after creating the object, before any memory is allocated for the object. The handler checked whether a page size had already been configured without holding the rangelock. Two concurrent callers could both observe an unconfigured object and set conflicting page sizes, leaving the object in an inconsistent state. An unprivileged local user can exploit this race to escalate privileges.	7.8	More Details
CVE-2026-80700	In the Linux kernel, the following vulnerability has been resolved: drm/vmwgfx: validate external BO copy bounds for both stride paths vmw_external_bo_copy() trusts caller-supplied offsets, strides, and heights and operates on imported dma-buf vmaps: - The equal-stride memcpy() bound was clamped after subtracting the offsets from dst_size and src_size; an offset larger than the BO size wraps the unsigned subtraction to a huge value and the resulting memcpy() runs off the end of the vmap. dst_stride * height is also a u32 multiplication that can overflow. - The non-equal-stride row-by-row path had no bound at all. The loop touches bytes through offset + (height - 1) * stride + width_in_bytes, with only a WARN_ON(dst_stride < width_in_bytes), and could likewise step past the end of either mapping. The offsets and strides are derived from STDU/SOU plane state, so a configured CRTC submitting a crafted atomic commit on an imported framebuffer can reach this path. Validate the exact row-copy endpoint against each BO's size up front using check_mul_overflow() and check_add_overflow(). Use the bulk memcpy() path only when width_in_bytes covers the whole stride; otherwise copy one row at a time so partial-row updates near the bottom of a framebuffer remain valid. Also reject zero strides and stride < width_in_bytes, both of which the row-by-row path cannot represent safely.	7.8	More Details
CVE-2026-80702	In the Linux kernel, the following vulnerability has been resolved: drm/vmwgfx: fix guest_memory_dirty bitfield clobbered as size Two sites in vmwgfx_resource.c assign boolean literals to res->guest_memory_size, which is an unsigned long allocation-size field; the intended target is the adjacent res->guest_memory_dirty bitfield. After the assignments the field holds 0 or 1 instead of the resource's MOB allocation size: - vmw_resource_release() writes 0 (false), and - vmw_resource_unbind_list() writes 1 (true). Subsequent revalidation paths read guest_memory_size when computing the dirty page range (vmw_bo_dirty_transfer_to_res()) and the buffer allocation size (vmw_resource_buf_alloc()), producing zero-length walks or wrap-around ranges that read or write past the MOB bitmap. The dirty-tracking intent of the original code (mark the resource as dirtied since the last sync) is also lost, since guest_memory_dirty is never updated. Rename both assignments to guest_memory_dirty.	7.8	More Details
CVE-2026-58097	mp_SetEnddisc() copied a user-supplied PSN endpoint value without length validation, allowing a buffer overflow via the ppp(8) command interface. A local user with access to the ppp(8) command interface can crash ppp(8) or potentially execute arbitrary code as root.	7.8	More Details
CVE-2026-34674	Substance3D - Sampler versions 5.1.3 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-78237	Insufficient input validation in ABR allows a low-privileged user to inject malicious entries into the sudoers file, resulting in persistent root access that remained effective after the ABR session ended.	7.8	More Details
	In the Linux kernel, the following vulnerability has been resolved: can: softing: fw_parse(): validate firmware record spans fw_parse() reads a fixed record header, a firmware-provided payload, and a trailing checksum without knowing the end of the firmware blob. A truncated record can therefore make those reads exceed		

CVE-2026-80706	the blob. The same record also supplies addresses and lengths for writes into DPRAM. The generic loader uses wrap-prone mixed signed arithmetic for its bounds check, while the application loader does not bound the staging copy at all. Pass the firmware end to the parser and validate the full source record. Use a signed wide offset for generic DPRAM records and validate the application staging span against the mapped DPRAM before copying.	7.8	More Details
CVE-2026-80710	In the Linux kernel, the following vulnerability has been resolved: s390/dasd: Fix undersized format-check buffer fmt_buffer_size in dasd_eckd_check_device_format() is declared as int, even though one of the multiplicands, sizeof(struct eckd_count), is a size_t. The expression trkcount * rpt_max * sizeof(struct eckd_count) is therefore correctly evaluated at 64-bit width, but the result is silently truncated when it is stored back into the 32-bit fmt_buffer_size variable. For a sufficiently large track range (start_unit/stop_unit are caller-controlled) this truncation yields a buffer size far smaller than the number of tracks actually requested. kzalloc() then succeeds with an undersized allocation, while the subsequent channel program build still operates on the untruncated track count and writes past the end of that buffer. Compute the buffer size with check_mul_overflow() and keep it in a size_t, so that a value that no longer fits results in -EINVAL instead of a silently truncated allocation size.	7.8	More Details
CVE-2026-19702	Improper neutralization of special elements used in an OS command ('OS command injection') vulnerability in TÜBİTAK BİLGEM Software Technologies Research Institute Pardus Boot Repair allows OS Command Injection. This issue affects Pardus Boot Repair: from 1.0.7 before 1.0.8.	7.8	More Details
CVE-2026-80522	In the Linux kernel, the following vulnerability has been resolved: crypto: tegra - fix rctx->cryptlen calculation in tegra_gcm_do_one_req() Perform rctx->cryptlen calculation in tegra_gcm_do_one_req() the same way it is done in tegra_ccm_crypt_init(). The current formulae may lead to a crash if a caller does not call tegra_gcm_setauthsize() and so ctx->authsize remains zero. Then a decrypt operation with incorrect rctx->cryptlen will lead to a write beyound rctx->dst_sg buffer. As a follow-up cleanup delete struct tegra_aead_ctx->authsize field since it appears to be completely unused. Also simplify tegra_ccm_setauthsize() and tegra_gcm_setauthsize() functions respectively.	7.8	More Details
CVE-2026-13732	A flaw was found in GDB's STABS debug format parser. The read_member_functions() function in gdb/stabsread.c contains a linked list removal bug in the code that separates destructor and non-destructor member functions of C++ classes. The bug causes the destructor entries to remain in the main function list while the list length counter is decremented, resulting in an out-of-bounds write when the function list is copied to its final allocated array. An attacker can craft an ELF binary with malicious .stab and .stabstr sections that triggers this out-of-bounds write when a user opens the file in GDB and performs any symbol-inspection operation such as setting a breakpoint. The inferior process does not need to be executed. Under controlled conditions, this was demonstrated to achieve execution of arbitrary commands within the GDB process.	7.8	More Details
CVE-2026-80559	In the Linux kernel, the following vulnerability has been resolved: Input: sur40 - fix input device registration ordering In sur40_probe(), input_register_device() was previously called early before the V4L2 video device and vb2_queue components were fully initialized. If userspace opened the input device immediately upon registration, sur40_open() would trigger and start the sur40_poll() worker thread. This worker thread invokes sur40_process_video() and accesses the uninitialized vb2_queue structure, leading to a data race and potential system crash. Furthermore, if V4L2 or video registration failed after input_register_device() succeeded, the error path fell through to calling input_free_device() on a successfully registered device instead of input_unregister_device(), corrupting input core state. Move input_register_device() to the very end of sur40_probe(). This ensures the V4L2 and video queue structures are fully initialized before polling can start, and naturally resolves the error path bug since input_free_device() is now only called when input registration has not yet occurred. To maintain strict LIFO (Last-In, First-Out) teardown ordering, also move input_unregister_device() to the very beginning of sur40_disconnect(). This guarantees that the input polling worker thread is stopped before V4L2 video components or control handlers are unregistered.	7.8	More Details
CVE-2026-80556	In the Linux kernel, the following vulnerability has been resolved: mmc: atmel-mci: Fix use-after-free in atmci_remove due to race condition In atmci_probe, &host->bh_work is bound with atmci_work_func, and atmci_interrupt, atmci_timeout_timer and atmci_dma_complete can all queue this work on system_bh_wq. If we remove the module, atmci_remove makes cleanup and the memory allocated for host with devm_kzalloc() is released after the remove callback returns, while the work mentioned above may still be pending or running. The sequence of operations that may lead to a UAF bug is as follows: CPU0 CPU1 | atmci_interrupt | queue_work(system_bh_wq, | &host->bh_work) atmci_remove | atmci_cleanup_slot(...) | atmci_writel(host, ATMCI_IDR, ~0UL) | timer_delete_sync(&host->timer) | dma_release_channel(host->dma.chan) | free_irq(platform_get_irq(pdev, 0), host) | | atmci_work_func | // use host // devm resources released after | // remove returns, host is freed | | // use host (use-after-free) Fix it by canceling the work after all the sources that can schedule it (IRQ handler, timeout timer and DMA completion callback) have been stopped, and before proceeding with the remaining cleanup in atmci_remove.	7.8	More Details
CVE-2026-57170	Compliance-trestle (Trestle) is a Python SDK and command-line tool for managing OSCAL compliance documents. In versions prior to 3.12.4 and 4.0.0 through 4.0.3, the custom Jinja2 include tags mdsection_include and md_clean_include re-parse the content of an included Markdown file as Jinja2 template code in a non-sandboxed environment, allowing server-side template injection that can lead to arbitrary code execution. The MDSectionInclude and MDCleanInclude tags in Trestle/core/jinja/tags.py pass included file content to Parser(self.environment, ...).parse(), splicing it into the host template's compilation, and the environment is a plain jinja2.Environment rather than a SandboxedEnvironment, so any expressions	7.8	More Details

	in the file are evaluated with full access to the usual SSTI gadget chain. Because Trestle's Markdown writers emit OSCAL prose and component-description fields verbatim, applying delimiter neutralization only to parameter tables, attacker-controlled OSCAL data such as a control statement, part prose, or component description containing Jinja2 syntax flows into an included Markdown file and is executed when the include tag re-parses it. This issue is fixed in version 4.1.0.		
CVE-2026-80582	In the Linux kernel, the following vulnerability has been resolved: drm/shmem_helper: Check VMA boundaries for PMD mappings In the ->huge_fault handler do not install a PMD huge page mapping if the huge page exceeds the boundaries of the VMA. All other ->huge_fault handlers have similar checks and the resulting mapping will trigger a VM_BUG_ON_VMA() if it ever reaches copy_pmd_range().	7.8	More Details
CVE-2026-80580	In the Linux kernel, the following vulnerability has been resolved: fbdev: bound mode sysfs output to the sysfs buffer mode_string() uses snprintf() which can return a value larger than the remaining buffer space. show_modes() accumulates the return value into i without checking whether i has reached PAGE_SIZE, causing the offset to advance past the sysfs buffer if the modelist is long enough. Add a size parameter to mode_string() and use scnprintf() to return only the bytes actually written. Add an early return when offset already exceeds the buffer. In show_modes(), stop accumulating once the buffer is full.	7.8	More Details
CVE-2026-80579	In the Linux kernel, the following vulnerability has been resolved: fbdev: clear fb_info->mode before deleting a videomode fb_set_var() can delete a mode from info->modelist when userspace passes FB_ACTIVATE_INV_MODE through FBIOPUT_VSCREENINFO. The code checks that the mode being deleted is not the current info->var and that fbcon is not using it, but it does not check fb_info->mode. fb_info->mode may still point into the modelist entry being deleted. If the entry is freed, later mode sysfs reads through show_mode() can dereference a stale pointer. Clear fb_info->mode before calling fb_delete_videomode() when it matches the mode being removed.	7.8	More Details
CVE-2026-80575	In the Linux kernel, the following vulnerability has been resolved: Input: cs40l50-vibra - validate custom data from user space cs40l50_add() copies the custom data of an FF_PERIODIC/FF_CUSTOM effect straight from the ff_effect the user passed to EVIOCSFF, without requiring it to hold anything: work_data.custom_data = memdup_array_user(periodic->custom_data, periodic->custom_len, sizeof(s16)); work_data.custom_len = periodic->custom_len; The driver then reads two words out of that buffer: custom_data[0] as the waveform bank in cs40l50_effect_bank_set(), and custom_data[1] as the index within the bank in cs40l50_effect_index_set(). Neither read is covered by a length check, and custom_len is fully user controlled: - custom_len == 0 makes memdup_array_user() call memdup_user() with a length of zero, which returns ZERO_SIZE_PTR rather than an error, so custom_data[0] dereferences it. - custom_len == 1 allocates two bytes. A bank of ROM or RAM keeps effect->type out of the OWT case, and custom_data[1] is then read one word past the allocation. The bank value itself is also mishandled. It is masked with CS40L50_CUSTOM_DATA_MASK (0xffff) but stored in an s16, so a custom_data[0] of 0x8000 or above wraps to a negative value that passes the "bank_type >= CS40L50_WVFRM_BANK_NUM" test. cs40l50_effect_index_set() indexes vib->dsp.banks[] with it before the switch statement's default case gets a chance to reject it: base_index = vib->dsp.banks[effect->type].base_index; max_index = vib->dsp.banks[effect->type].max_index; Require the two words the driver reads to be present, and hold the masked bank in a u32 so the existing upper-bound test covers the whole range. The da7280 haptic driver already range checks custom_len this way.	7.8	More Details
CVE-2026-80572	In the Linux kernel, the following vulnerability has been resolved: Input: byd - synchronize timer deletion before freeing private data byd_disconnect() uses timer_delete() before freeing the driver's private data. This does not wait for a running byd_clear_touch() callback, which dereferences the private data and its psmouse pointer. A callback racing with disconnect can therefore access the private data after it has been freed. The timer can also still be re-armed by byd_process_byte() while the disconnect is in progress. Use timer_shutdown_sync() before freeing the private data: it waits for a running callback and turns any later re-arm attempt into a no-op.	7.8	More Details
CVE-2026-80570	In the Linux kernel, the following vulnerability has been resolved: Input: synaptics-rmi4 - zero report size on F54 work error In rmi_f54_work(), if an error occurs during report request or command verification, the code jumped directly to the 'error' label, bypassing the 'abort' label where f54->report_size was normally zeroed out. This left f54->report_size containing its previous successful payload size. If a user then altered the V4L2 format to a smaller size, and a subsequent run failed, rmi_f54_buffer_queue() would copy the stale, larger payload size into the shrunken V4L2 buffer, causing a heap buffer overflow. Fix this by merging the 'abort' and 'error' labels into a single 'out' exit path, and ensuring that f54->report_size is always set to 0 on failure by checking for error and zeroing the local report_size first.	7.8	More Details
CVE-2026-80569	In the Linux kernel, the following vulnerability has been resolved: Input: synaptics-rmi4 - bound the F54 report size to the allocated buffer rmi_f54_work() reads a diagnostics report from the device into f54->report_data, sizing the transfer with rmi_f54_get_report_size(): report_size = rmi_f54_get_report_size(f54); ... for (i = 0; i < report_size; i += F54_REPORT_DATA_SIZE) { int size = min(F54_REPORT_DATA_SIZE, report_size - i); ... rmi_read_block(.., f54->report_data + i, size); } report_data is allocated once at probe from F54's own electrode counts (array3_size(f54->num_tx_electrodes, f54->num_rx_electrodes, sizeof(u16))), but rmi_f54_get_report_size() computes the size from drv_data->num_*_electrodes when those are set, i.e. from the F55 function's electrode counts. Both counts come straight from device queries (F54 and F55 each report up to 255 electrodes) and nothing constrains the F55 counts to the F54 ones. A malicious or malfunctioning RMI4 device that reports larger F55 electrode counts than its F54 counts makes report_size exceed the allocation, so the read loop writes past report_data (and the V4L2 dequeue memcpy() then reads past it). On conforming hardware the F55 configured electrodes are a subset of the	7.8	More Details

	F54 physical electrodes, so report_size never exceeds the buffer and well-behaved devices are unaffected. Record the allocation size and reject a report that does not fit, mirroring the existing zero-size check.		
CVE-2026-80568	In the Linux kernel, the following vulnerability has been resolved: Input: synaptics-rmi4 - block s_input when F54 queue is busy Changing the input (diagnostic report type) mid-stream changes the report size. Since V4L2 buffers are allocated based on the size at stream start, changing the input while streaming could lead to a heap buffer overflow if the new size is larger than the allocated buffers. Prevent this by blocking VIDIOC_S_INPUT with -EBUSY if the V4L2 queue is busy (streaming).	7.8	More Details
CVE-2026-82457	su-exec through 0.3 fails to validate numeric user and group identifiers parsed with strtol before assigning to uid_t and gid_t, allowing truncation of out-of-range values to zero. Attackers can supply large numeric identifiers that truncate to root's identifier, causing su-exec to execute target programs with root privileges instead of intended unprivileged accounts.	7.8	More Details
CVE-2026-80565	In the Linux kernel, the following vulnerability has been resolved: crypto: qce - fix error path in devm_qce_register_algs If ops->register_algs() fails, the error path repeatedly calls the same ops->unregister_algs() from the failed registration. Use the loop index to unregister the previously registered algorithms instead.	7.8	More Details
CVE-2026-80560	In the Linux kernel, the following vulnerability has been resolved: openrisc: signal: do not restore privileged SR bits on sigreturn restore_sigcontext() copies the whole supervision register (SR) from the signal frame and only clears SPR_SR_SM before the value is reloaded into the hardware SR (through ESR and l.rfe) on the return to user space. All other SR bits are left under user control. An unprivileged task can thus return from a signal handler through a crafted sigframe that clears SPR_SR_DME. With the data MMU disabled the CPU performs no translation or protection on data accesses, so the task gains read and write access to arbitrary physical memory, a local privilege escalation. SPR_SR_IME, SPR_SR_SUMRA, SPR_SR_LEE, SPR_SR_EPH and the cache-enable bits are exposed the same way. The ptrace GPR regset already refuses any change to SR for exactly this reason. Restore only the arithmetic flag bits (F, CY, OV) from the signal frame and take every privileged control bit from the SR the kernel saved on signal entry. Verified with qemu-system-or1k -M or1k-sim: before this change an unprivileged PoC clears SPR_SR_DME in rt_sigreturn and writes a marker to physical address 0x03000000 (beyond the kernel's mem=32M); afterwards the same PoC receives SIGSEGV and physical memory is unchanged.	7.8	More Details
CVE-2026-58091	The implementation of this ioctl attempts to acquire locks on all channels in a sync group. If locking a channel would block, it releases the sync group list lock and sleeps. Upon reawakening, it is possible that the sync group structure is freed, but the implementation did not handle this possibility. On a system with a multiple audio devices, an unprivileged local user can exploit this use-after-free to escalate privileges.	7.8	More Details
CVE-2026-80709	In the Linux kernel, the following vulnerability has been resolved: s390/zcrypt: Fix wrong domain value verification with EP11 CPRBs There is a wrong upper limit check for the domain value when an EP11 CPRB is processed for sending to a crypto card. This check is only active on custom device nodes but may lead to access heap memory behind perms->adm when an administrative CPRB is sent. Add correct limit (AP_DOMAINS = 256) checking to fix this.	7.8	More Details
CVE-2026-80546	In the Linux kernel, the following vulnerability has been resolved: s390/zcrypt: Improve CCA CPRB length and overflow checks The xcrb_msg_to_type6cprb_msgx() function lacks proper input validation, creating security vulnerabilities: 1. Integer overflow after CEIL4 alignment: Signed int variables could overflow during 4-byte boundary alignment, causing undersized buffer allocations or incorrect bounds checking. 2. Missing minimum size validation: The CPRBX structure is copied from userspace without verifying sufficient buffer length. Undersized buffers cause uninitialized memory access when reading structure fields like cprbx.cprb_len and cprbx.domain. 3. Arithmetic overflow in sum calculations: Adding control block and data block sizes could overflow, bypassing size checks and enabling buffer overflows. Fix by using size_t for length calculations, adding U32_MAX boundary checks after alignment, validating minimum control block size before copying from userspace, and detecting sum calculation overflows.	7.8	More Details
CVE-2026-80544	In the Linux kernel, the following vulnerability has been resolved: s390/zcrypt: Improve EP11 CPRB domain handling with ASN.1 parsing The zcrypt_msgtype6_send_ep11_cprb() function uses fragile struct overlays to access and modify the domain field in the EP11 CPRB payload, creating maintainability and security concerns: 1. Struct overlay approach (pld_hdr) assumes fixed payload structure and doesn't validate the actual ASN.1 encoding. 2. Complex length format detection logic is error-prone and doesn't properly validate bounds at each parsing step. 3. Direct struct member access bypasses proper ASN.1 validation. Fix by replacing struct overlays with explicit ASN.1 parsing that validates each field (payload tag/length, function tag/length/value, optional domain tag/length/value) with proper bounds checking at every step. Add asn1_int_encode() helper function to safely write integer values with correct endianness conversion. This makes the code consistent with the validation pattern introduced with the rework of the xcrb_msg_to_type6_ep11cprb_msgx() function.	7.8	More Details
CVE-2026-58090	The SOCK_STREAM receive path in the unix socket implementation failed to fully detach control messages from the socket buffer before processing them. Some error paths would free those messages, leaving freed data mbufs in the receive socket buffer. An unprivileged local user can exploit this use-after-free to escalate privileges.	7.8	More Details
	In the Linux kernel, the following vulnerability has been resolved: xfs: fix off-by-one in rtrefcount btree root level validation xfs_rtrefcountbt_compute_maxlevels() sets mp->m_rtrefc_maxlevels = min(d_maxlevels,		

CVE-2026-80537	r_maxlevels) + 1; where the trailing "+ 1" already accounts for the inode-root level, so the deepest valid on-disk root level is m_rtrefc_maxlevels - 1 and a cursor must satisfy bc_nlevels <= bc_maxlevels (= m_rtrefc_maxlevels). The two on-disk validation paths, xfs_rtrefcountbt_verify() and xfs_iformat_rtrefcount(), check the root level with ">" instead of ">=", so a crafted rtreflink (metadir + realtime + reflink) image whose /rtgroups/N.refcount inode has bb_level == m_rtrefc_maxlevels is accepted on mount. xfs_rtrefcountbt_init_cursor() then sets bc_nlevels = bb_level + 1, exceeding bc_maxlevels by one. Since the xfs_rtrefcountbt_cur slab object is sized for exactly bc_maxlevels entries, the first btree op on such a cursor indexes bc_levels[m_rtrefc_maxlevels] past the end of the object. This is reached by the first rtrefcount cursor built after mount, via log/CoW recovery (xfs_reflink_recover_cow() during xfs_mountfs()) or an FS_IOC_GETFSMAP over the realtime device. Reject a root level equal to m_rtrefc_maxlevels, matching the ">=" form already used by the sibling data-device refcount/rmap verifiers and the in-memory rtrmap verifier. BUG: KASAN: slab-out-of-bounds in xfs_btree_lookup (fs/xfs/libxfs/xfs_btree.c:2101) Write of size 2 at addr ffff888018391658 by task exploit/144 xfs_btree_lookup (fs/xfs/libxfs/xfs_btree.c:2101) xfs_btree_query_range (fs/xfs/libxfs/xfs_btree.c:5308) xfs_refcount_recover_cow_leftovers (fs/xfs/libxfs/xfs_refcount.c:2113) xfs_reflink_recover_cow (fs/xfs/xfs_reflink.c:1085) xlog_recover_finish (fs/xfs/xfs_log_recover.c:3551) xfs_mountfs (fs/xfs/xfs_mount.c:1158) xfs_fs_fill_super (fs/xfs/xfs_super.c:1940) get_tree_bdev_flags (fs/super.c:1634) vfs_get_tree (fs/super.c:1694) path_mount (fs/namespace.c:4161) __x64_sys_mount (fs/namespace.c:4367) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:121) The buggy address belongs to the cache xfs_rtrefcountbt_cur of size 216 The buggy address is located 8 bytes to the right of allocated 216-byte region [ffff888018391578, ffff888018391650) Kernel panic - not syncing: Fatal exception	7.8	More Details
CVE-2026-80540	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix UVD decode image min size calculation This needs to use pitch instead of width. Also reject pitch over 4096 to avoid overflow. (cherry picked from commit b41c8cb12e202b220353332ab87dc01a11f69304)	7.8	More Details
CVE-2026-80541	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: validate GEM_CREATE domain combinations AMDGPU_GEM_CREATE checked domain bits against AMDGPU_GEM_DOMAIN_MASK, but did not validate domain combinations. Userspace could combine CPU|GTT|VRAM with DOORBELL, GDS, GWS, or OA, making amdgpu_bo_placement_from_domain() exceed AMDGPU_BO_MAX_PLACEMENTS and hit BUG_ON(). Allow combinations only within CPU/GTT/VRAM, and require non-CPU/GTT/ VRAM domains to be specified one at a time. Return -EINVAL for invalid combinations in amdgpu_gem_create_ioctl(). v2: Rename helper from amdgpu_gem_domain_valid() to amdgpu_gem_are_domains_valid() (Christian) (cherry picked from commit db39852d0c39843cb02048dfb47e4b8c703e9080)	7.8	More Details
CVE-2026-82474	Sudo through 1.9.17p2 fails to apply intercept policy checks to the execveat system call in ptrace-based intercept mode. Users permitted to run specific commands can execute denied programs by calling execveat directly or through fexecve, bypassing policy enforcement and logging.	7.8	More Details
CVE-2026-80545	In the Linux kernel, the following vulnerability has been resolved: s390/zcrypt: Improve EP11 CPRB length and overflow checks The xcrb_msg_to_type6_ep11cprb_msgx() function lacks proper input validation, creating security vulnerabilities: 1. Missing minimum size validation: The ep11_cprb structure and subsequent payload fields (pld_tag, pld_lenfmt) are copied from userspace without verifying sufficient buffer length. 2. Arithmetic overflow in length calculations: CEIL4 alignment could overflow, bypassing size checks and enabling buffer overflows. 3. The payload is asn1 encoded but the function just uses a simple c struct overlay to access some fields of the payload. Fix by using size_t for length calculations, adding U32_MAX boundary checks after alignment, and validating minimum request size and minimum reply size before copying from userspace. Do a very simple asn1 parsing of the payload up to the function value field.	7.8	More Details
CVE-2026-58089	When a process calls execve(2) to execute a setuid or setgid image, hwpmc(4) is supposed to detach PMCs owned by unprivileged processes. An inverted check meant that this scenario was not handled properly. An unprivileged local user who has attached PMCs to a process can continue monitoring it after the process executes a setuid or setgid binary, contrary to the intended policy.	7.8	More Details
CVE-2026-57171	Compliance-trestle (Trestle) is a Python SDK and command-line tool for managing OSCAL compliance documents. In versions before 3.12.4 and versions 4.0.0 through 4.0.3, the catalog-generate, profile-generate, and ssp-generate author commands write generated Markdown to an attacker-influenced output path without path-traversal validation, allowing arbitrary file write outside the Trestle workspace. These commands join the user-supplied output argument onto the Trestle root and write to the result, but guard it only with an is_directory_name_allowed() task-name-collision check rather than the PathSecurityValidator.validate_local_path() guard used by the jinja command, so an absolute path or one containing traversal sequences escapes the workspace and writes files under an attacker-chosen location as the invoking process owner. The security boundary is crossed when a trusted CI job, shared service, or wrapper derives the output argument from repository-controlled, tenant-controlled, or otherwise untrusted data while expecting output to stay inside the workspace. When --force-overwrite is used, the selected output directory is first recursively deleted, extending the primitive to destruction of an attacker-chosen directory tree and enabling indirect code execution by overwriting files a pipeline later runs. This issue is fixed in versions 3.12.4 and 4.1.0.	7.7	More Details
CVE-2026-79750	MCPHub is a unified hub for centrally managing and dynamically orchestrating multiple MCP servers/APIs into separate endpoints with flexible routing strategies. Prior to version 1.0.30, MCPHub scopes non-admin users to servers they own (list views and config edits enforce ownership), but the tool-execution API does not. Any authenticated non-admin user can invoke tools on MCP servers owned by other users — servers	7.7	More Details

	they cannot even see in GET /api/servers. Because connected MCP servers carry real capability (filesystem, HTTP fetch, cloud APIs with the owner's keys), this is cross-tenant compromise: demonstrated arbitrary host file read (/etc/passwd, another user's secrets) and SSRF. This issue has been patched in version 1.0.30.		
CVE-2026-47879	Spring Cloud Gateway JsonToGrpcGatewayFilterFactory allows arbitrary Spring Resource locations for defining the proto descriptor. Spring Cloud Gateway 5.0.0 - 5.0.2 Spring Cloud Gateway 4.3.0 - 4.3.5 Spring Cloud Gateway 4.0.0 - 4.2.9 Spring Cloud Gateway 3.1.13 and earlier	7.7	More Details
CVE-2026-61792	Weblate is a web-based continuous localization platform used to manage software translations. In versions prior to 2026.7, a project administrator can read files outside their repository through the App store metadata download feature, which resolves attacker-influenced paths without adequately confining them to the repository. This is an incomplete fix for CVE-2026-34242, whose original patch failed to fully prevent the path traversal, allowing the arbitrary file read to persist. A user with project-administrator privileges can therefore disclose the contents of files on the Weblate host that lie outside the project's repository. This issue is fixed in version 2026.7.	7.7	More Details
CVE-2026-75797	The AI Engine WordPress plugin before 3.7.2 does not confine a caller-supplied URL when mapping it to a local filesystem path before reading the file and forwarding its contents to an external service, allowing users with a subscriber-level account to read arbitrary files from the server and exfiltrate them off-host. Reaching the issue at subscriber level requires a non-default public API feature to be enabled; otherwise the same issue is reachable by an administrator, which on multisite allows a non-super subsite administrator to read the network-shared configuration and its secrets.	7.7	More Details
CVE-2026-53553	Goploy is an open-source automation deployment system. Prior to version 1.18.0, a severe path traversal vulnerability exists in its backend API endpoints, specifically /deploy/fileDiff (File Compare), when handling file paths provided by the client. This issue has been patched in version 1.18.0.	7.7	More Details
CVE-2026-61617	Wings is the server control plane for the Pterodactyl game-server management panel. In versions up to and including 1.13.2, the SFTP write path does not enforce a server's disk quota during a transfer, allowing a tenant with SFTP write access to a single server to exhaust the host node's physical disk and take down every server on it. Wings checks available space only once, as a boolean, when the write handle is opened, using a stale cached usage value and without knowing the size of the incoming data, and it then returns a raw, unaccounted file handle that is never re-checked as the transfer proceeds. A single upload can therefore be written without bound, far beyond the configured disk limit, until the node's disk is full, and because a server stopped for exceeding its limit is not treated as suspended, SFTP writes are still accepted even after the quota is already exceeded. This issue is fixed in version 1.13.3.	7.7	More Details
CVE-2026-81576	If configured as a server, CodeMeter Runtime before versions 8.41a and 9.10 issues handles per connection and relies on a cryptographically weak SID as sole authenticator. An attacker can brute-force the SID, recover another session's handle number, and read license information belonging to another handle.	7.7	More Details
CVE-2026-82242	Budibase versions before 3.41.3 contain a missing authorization vulnerability in the POST /api/resources/duplicate endpoint that allows authenticated builders to inject tables, automations, queries, and screens into any other application without holding any role in the destination workspace. Attackers can inject resources by specifying an arbitrary destination workspace ID in the request body, then trigger injected automations with outgoing webhooks to exfiltrate data from victim applications.	7.7	More Details
CVE-2026-16600	The SmartAIPress WordPress plugin through 1.2.0 does not perform a capability check on one of its AJAX actions and does not validate a user-supplied URL before fetching it server-side, allowing users with subscriber-level access and above to make the site retrieve arbitrary internal or external URLs and read the response, resulting in a full-read Server-Side Request Forgery.	7.7	More Details
CVE-2026-81679	OpenRemote versions before 1.28.0 contain a cross-realm information disclosure vulnerability in the Notification REST API that allows per-realm tenant administrators to read all tenants' sent notifications including message bodies. Attackers with read:admin credentials in one realm can submit a zero-parameter GET request to the notification endpoint to retrieve sensitive notification metadata and message content from all realms.	7.7	More Details
CVE-2026-82871	ToolJet before v3.16.208 fails to validate organization membership in database read routes, allowing any authenticated user to access other organizations' table schemas and row data. Attackers can supply arbitrary organization IDs in URL parameters to list tables, retrieve column definitions, and execute join queries to read actual stored data from victim organizations.	7.7	More Details
CVE-2026-41012	Traffic interception vulnerability in BOSH Director vCenter CPI allows attackers positioned between BOSH Director and vCenter to impersonate vCenter REST API and capture administrator credentials via HTTP Basic auth, leading to complete virtualization infrastructure takeover. An attacker who can intercept traffic between the BOSH Director and vCenter can establish a malicious server impersonating the vCenter REST API. When the BOSH Director makes CPI calls to perform routine cloud infrastructure operations, the attacker captures the vCenter administrator username and password transmitted via HTTP Basic authentication. The vulnerability stems from insufficient authentication security in the communication protocol between BOSH Director and vCenter. While HTTPS may be used, the lack of proper certificate validation and pinning allows attackers to successfully impersonate vCenter endpoints. Because vCenter credentials typically grant full administrative control over the entire virtualization estate, successful credential capture yields complete takeover of every VM, datastore, and network the CPI manages. This exposure exists on every CPI call	7.7	More Details

	(including routine deployment operations, not just when tags are configured) and cannot be mitigated by supplying a CA certificate alone. The attack impacts all infrastructure managed by the compromised vCenter instance, potentially affecting hundreds or thousands of VMs across multiple deployments and environments.		
CVE-2026-75889	Grafana Alloy's prometheus.operator.servicemonitors component allows a user who can create or modify ServiceMonitor resources in a watched namespace to specify an arbitrary local file through bearerTokenFile. Alloy reads the file and sends its contents as a bearer token to an attacker-controlled scrape endpoint. This may disclose files accessible to the Alloy process, including its projected Kubernetes service account token, potentially granting the attacker Alloy's Kubernetes permissions. Exploitation requires ServiceMonitor write access and lower privileges than Alloy's service account.	7.7	More Details
CVE-2026-82869	ToolJet Database versions before v3.16.44 contain a privilege escalation vulnerability in the join_tables endpoint that grants JOIN_TABLES ability to all authenticated users without role or workspace membership validation. Attackers can read arbitrary ToolJet Database tables from any workspace by supplying victim workspace identifiers in the request path while authenticating with their own workspace credentials.	7.7	More Details
CVE-2026-77017	The Workeera WordPress plugin before 1.0.6 does not restrict which profile values a candidate may submit, nor confine the stored file location to an allowed directory before serving it, allowing users with a role as low as subscriber to read arbitrary files on the server, including its configuration file and authentication secrets.	7.7	More Details
CVE-2026-81490	A database user able to create a view in a namespace that MongoDB Connector for BI samples can cause the schema-sampling routine to stop functioning by defining a view whose evaluation reliably fails. The sampling logic classifies the resulting server message as transient and, after the configured retries are exhausted, proceeds without a valid result, ending the schema refresh routine. The mongosqld process continues running without a usable schema, so SQL clients are unable to obtain results until an operator removes the view or excludes its namespace from sampling.	7.7	More Details
CVE-2026-29988	A cleartext transmission of sensitive information vulnerability in the NFC interface of multiple Milesight IoT device models running affected firmware versions allows an unauthenticated attacker with physical proximity to retrieve LoRaWAN ABP NwkSKey and AppSKey values and D2D keys via an NFC read operation. The exposed keys can be used to decrypt LoRaWAN traffic, forge uplink and downlink frames, submit falsified sensor data, issue supported device commands, and cause subsequent legitimate frames to be rejected.	7.6	More Details
CVE-2026-40463	WaveSuite is affected by an insufficient role-based access control vulnerability in the CPB Log Files feature. Successful exploitation allows an authenticated low-privilege user to load pages restricted to higher-privilege roles by requesting the corresponding URL directly in the browser.	7.6	More Details
CVE-2026-59284	There is no allow list for property keys when Spring Cloud Commons writable /actuator/env is enabled. Spring Cloud Commons 5.0.0 - 5.0.2 Spring Cloud Commons 4.3.0 - 4.3.3 Spring Cloud Commons 4.0.0 - 4.2.6 Spring Cloud Commons 3.1.10 and earlier	7.6	More Details
CVE-2026-47666	Penpot is an open-source design and prototyping platform. In versions up to and including 2.14.3, Penpot is vulnerable to stored cross-site scripting through custom font family names, which are interpolated into a @font-face CSS rule and injected into the page as HTML without sanitization. Because the backend accepts an arbitrary font-family string and the frontend writes the resulting style through innerHTML, a name containing markup such as a closing style tag followed by a script can break out of the style element and execute JavaScript on the Penpot origin. The attack is passive: any team member who opens a file referencing the malicious font triggers script execution simply by rendering the page, allowing theft of session cookies, actions performed as the victim, and access to their files and projects. This issue is fixed in version 2.15.3.	7.6	More Details
CVE-2026-66155	A vulnerability has been identified in Element maps-ng V47 (All versions < V47.12.3), Element maps-ng V48 (All versions < V48.11.3), Element maps-ng V49 (All versions < V49.16.1). The si-map component does not properly neutralize user-controllable input of the points property that is used to render the tooltip label of map pins. This could allow an attacker to craft a malicious URL that, when loaded by a victim and the map pin is hovered over, executes arbitrary script code within the victim's browser session.	7.6	More Details
CVE-2026-38822	In openNDS before 11.0.0, the client_params.sh script, invoked by the openNDS daemon to serve the authenticated client status page, is vulnerable to OS command injection through crafted HTTP GET query parameter keys. An authenticated captive portal user can inject arbitrary shell commands by embedding semicolons in a URL query parameter name.	7.6	More Details
CVE-2026-77368	SeaweedFS is a distributed storage system for files and blobs. In version 4.39, the filer's TUS resumable-upload handler checks JWT allowed_prefixes scoping only when a session is created, letting a low-privilege tenant hijack another tenant's upload session to write content to filer paths their own token forbids. The HEAD, PATCH, and DELETE verbs that act on an existing session by its id never verify that the session's stored target path falls within the caller's allowed prefixes, so a tenant who obtains another upload's session identifier can PATCH attacker bytes into it and, on completion, have the file land at the victim's out-of-scope path. The same token can also DELETE other tenants' sessions and HEAD them to read upload progress and size, defeating the JWT prefix isolation. This vulnerability only affects deployments that configure filer JWT signing and have TUS uploads enabled. This issue is fixed in version 4.40.	7.6	More Details

CVE-2026-82017	IGEL OS 12 before 12.7.6 and IGEL OS 11 before 11.11.150 contain a boot registry parameter injection vulnerability that allows attackers with physical access to execute arbitrary Linux loader parameters by writing to an unencrypted and unsigned configuration area read by the signed bootloader. Attackers can inject malicious kernel command line parameters that execute with boot environment privileges without triggering TPM PCR measurement failures, as the attack does not modify the measured boot code.	7.6	More Details
CVE-2026-79938	Dell PowerProtect Cyber Recovery, versions prior to 20.3, contain an Improper Authentication vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Unauthorized access.	7.6	More Details
CVE-2026-82243	Budibase Server before 3.41.3 contains a server-side request forgery vulnerability in the datasource verify endpoint that allows builder-level users to supply arbitrary URLs without SSRF validation. Attackers can exploit this to leak internal CouchDB credentials by making requests to attacker-controlled servers, gaining full database access in cloud deployments.	7.6	More Details
CVE-2026-75005	Inefficient Algorithmic Complexity vulnerability in Apache APISIX. A single small request can pin a gateway worker at 100% CPU for an extended period in graphql-limit-count routes. This issue affects Apache APISIX: 3.17.0. Users are recommended to upgrade to version 3.18.0, which fixes the issue.	7.5	More Details
CVE-2026-19715	The WP OAuth Server (Login with WordPress) WordPress plugin before 6.3.1 does not restrict access to the debug log it writes, which is stored at a fixed and publicly reachable location, allowing unauthenticated users to read the OAuth tokens and authorisation codes it has issued as well as user records including password hashes when debug logging is enabled.	7.5	More Details
CVE-2026-80433	Subscriber Sensitive Data Exposure in SureFeedback Client Site <= 1.2.12 versions.	7.5	More Details
CVE-2026-80707	In the Linux kernel, the following vulnerability has been resolved: can: j1939: transport: j1939_session_fresh_new(): initialize receive buffer Zero the allocated buffer in j1939_session_fresh_new() to ensure it contains no residual data. While there is a potential performance impact if users allocate maximum sized ETP buffers, most real-world use cases are not noticeably affected since the maximum known buffer size is typically around 65K. [mkl: add Message-ID]	7.5	More Details
CVE-2026-80720	In the Linux kernel, the following vulnerability has been resolved: iomap: add a separate bio_set for iomap_split_ioend iomap_split_ioend can split bios that already come from iomap_ioend_bioset and thus deadlock when the bioset is exhausted. Add a separate bio_set to avoid this deadlock. Christian Brauner <brauner@kernel.org> says: Mark iomap_ioend_split_bioset static as it is only used in ioend.c, fixing the sparse warning reported by the kernel test robot.	7.5	More Details
CVE-2026-74848	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling') vulnerability in Apache APISIX. An attacker could make other clients receive attacker-chosen or other users' responses on serverless-plugin routes. This issue affects Apache APISIX: from 2.12.0 through 3.17.0. Users are recommended to upgrade to version 3.18.0, which fixes the issue.	7.5	More Details
CVE-2026-47893	A Spring WebFlux application that supports WebSocket connections may expose indirectly sensitive user information by including request headers in an exception reason. Spring Framework 7.0.0 - 7.0.8 Spring Framework 6.2.0 - 6.2.19 Spring Framework 6.1.0 - 6.1.28 Spring Framework 6.0.0 - 6.0.30 Spring Framework 5.3.0 - 5.3.49 Spring Framework 5.2.25.RELEASE and earlier	7.5	More Details
CVE-2026-80717	In the Linux kernel, the following vulnerability has been resolved: sctp: validate Adaptation Indication parameter length The Adaptation Layer Indication parameter contains a fixed 32-bit Adaptation Code Point after its parameter header. However, sctp_verify_param() accepts a header-only parameter because the generic parameter walker only requires the header to be present. sctp_process_param() then reads adaptation_ind beyond the declared parameter. When the malformed parameter is last in an INIT, the read starts at the receive skb tail, and the value is copied into the state cookie returned in the INIT ACK. This may disclose four receive-buffer tail bytes. Require the declared parameter length to match the fixed structure size and abort the association through the existing invalid parameter length path otherwise.	7.5	More Details
CVE-2026-80691	In the Linux kernel, the following vulnerability has been resolved: scsi: target: iblock: Fix wrong PR ops NULL check for PREEMPT/RELEASE In the iblock_execute_pr_out() function, PRO_PREEMPT, PRO_PREEMPT_AND_ABORT, and PRO_RELEASE all perform callback capability checks through ops->pr_clear. The error check allows unimplemented hooks to pass through the gate, resulting dereferencing a NULL function pointer. Check whether the hooks that need to be called are supported.	7.5	More Details
CVE-2026-47885	The PartEventHttpMessageReader in Spring WebFlux does not enforce the maxPartSize limit when maxInMemorySize is set to -1. Spring Framework 7.0.0 - 7.0.8 Spring Framework 6.2.0 - 6.2.19 Spring Framework 6.1.0 - 6.1.28	7.5	More Details
CVE-2026-47886	Applications that evaluate user-supplied Spring Expression Language (SpEL) expressions may be vulnerable to a Denial of Service (DoS) attack when the power operator (^) is used with a BigDecimal or BigInteger operand and a large exponent value. Spring Framework 7.0.0 - 7.0.8 Spring Framework 6.2.0 - 6.2.19 Spring Framework 6.1.0 - 6.1.28 Spring Framework 6.0.0 - 6.0.30 Spring Framework 5.3.0 - 5.3.49 Spring Framework 5.2.25.RELEASE and earlier	7.5	More Details
	A Spring RSocket application is exposed to a memory leak via a malformed SETUP frame. Spring Framework		

CVE-2026-47888	7.0.0 - 7.0.8 Spring Framework 6.2.0 - 6.2.19 Spring Framework 6.1.0 - 6.1.28 Spring Framework 6.0.0 - 6.0.30 Spring Framework 5.3.0 - 5.3.49 Spring Framework 5.2.0.RELEASE - 5.2.25.RELEASE	7.5	More Details
CVE-2026-47889	A WebFlux application running on the Jetty 12 Core reactive adapter serializes response cookies without the sameSite attribute. Spring Framework 7.0.0 - 7.0.8 Spring Framework 6.2.0 - 6.2.19	7.5	More Details
CVE-2026-78137	The StoreGrowth WordPress plugin before 2.1.2 does not validate a browser-supplied product price on two of its unauthenticated actions, allowing unauthenticated attackers to add a product to the cart at an arbitrary, attacker-chosen price that carries through to the checkout total when the BOGO offer feature is enabled.	7.5	More Details
CVE-2026-67560	Bendix EC80 Brake ECU is vulnerable to a stack-based buffer overflow, which may allow an attacker to crash the ECU. A crafted payload can then be used to remotely execute arbitrary code or inject arbitrary CAN bus traffic. This could cause the loss of the ABS function, steering assist, speedometer, and shifting.	7.5	More Details
CVE-2026-80646	In the Linux kernel, the following vulnerability has been resolved: ipv6: guard against possible NULL deref in __in6_dev_stats_get() dev_get_by_index_rcu() could return NULL if the original physical device is unregistered. Found by Sashiko.	7.5	More Details
CVE-2026-30073	An issue in the NssaiAvailabilitySubscriptionCreate component of free5gc v4.0.1 allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	7.5	More Details
CVE-2026-30067	An issue in the complexQueryFilterSubprocess function in the NRF Discovery service of free5gc v4.0.1 allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2026-30068	Improper input validation in the HandleUpdate function (/sbi/parameter_provision.go) of free5gc v4.0.1 allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2026-30069	A NULL pointer dereference in the UDMC registration handler component of free5gc v4.0.1 allows attackers to cause a Denial of Service (DoS) via supplying crafted payload.	7.5	More Details
CVE-2026-30070	An issue in the HandleGetSharedData function of free5gc v4.0.1 allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2026-30071	An issue in the RechargePut function of free5gc v4.0.1 allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2026-30072	A NULL pointer dereference in the CDR processing path of free5gc v4.0.1 allows attackers to cause a Denial of Service (DoS) via supplying crafted payload.	7.5	More Details
CVE-2026-5680	A flaw was found in Undertow. A remote attacker could exploit this vulnerability by sending specially crafted WebSocket messages with permessage-deflate negotiated. This could lead to excessive memory consumption due to the PerMessageDeflateFunction.largerBuffer() method using exponential doubling, resulting in a Denial of Service (DoS) for the affected application.	7.5	More Details
CVE-2026-81575	If configured as a server, CodeMeter Runtime before versions 8.41a and 9.10 accepts requests with opcode 0x5e, which contain the data length and the data itself. Missing bounds checking on the data length value can lead to out of bounds reads, causing a segmentation fault that ultimately crashes the CodeMeter Runtime.	7.5	More Details
CVE-2026-78002	A flaw was found in rsyslog. An unauthenticated remote attacker can trigger a heap buffer overflow in the RainerScript `replace()` function by sending specially crafted syslog messages. This vulnerability arises from an incorrect buffer size calculation during string replacement, causing memory corruption. Successful exploitation can lead to a denial of service (DoS) for the affected system.	7.5	More Details
CVE-2026-80212	An issue was discovered in the resolv gem before 0.7.2 for Ruby. Resolv::DNS::Resource.get_class, Resolv::DNS::Resource::Generic.create, and Resolv::DNS::SvcParam::Generic.create generate a new class for each unknown DNS resource record (type, class) pair, or each unknown SvcParamKey, encountered while decoding a response. Each generated class was permanently registered both as a constant on Resource (or SvcParam::Generic) and as an entry in a class-lookup hash (ClassHash), and thus the class remained reachable through that constant after the response was discarded. Type and class are each 16-bit values, and thus an attacker controlling DNS responses (a spoofed response, or a malicious or hijacked upstream DNS server) has roughly 2^32 distinct (type, class) pairs to choose from. A single response of a few hundred kilobytes carrying tens of thousands of distinct unknown types permanently grows process memory by tens of megabytes; repeated responses accumulate without bound and are never reclaimed by garbage collection, because the constant keeps each class alive. Any code path that calls Resolv::DNS::Message.decode on attacker-influenced DNS responses is affected. resolv is a default gem, and thus this is reachable from a plain Ruby installation without any additional dependency.	7.5	More Details
CVE-2026-81335	Baserow dispatches an Application Builder data source without acting on the result of its permission check. The dispatch and record-name views in backend/src/baserow/contrib/builder/api/data_sources/views.py are declared with a permission class that admits any caller, so a request carrying no credential reaches the handler. DataSourceService.dispatch_data_sources in backend/src/baserow/contrib/builder/data_sources/service.py then calls check_multiple_permissions without asking it to raise, and neither stores nor examines the mapping of denials it returns, so a denied check leaves execution to continue and the data source is dispatched whatever the caller's identity. The dispatch	7.5	More Details

	runs with the integration's own credentials, so an unauthenticated request naming a data source receives the rows and fields that source reads. Identifiers are small integers and can be enumerated. Version 2.3.1 passes raise_exception to the same call.		
CVE-2026-81678	AVideo before 24.0 contains a server-side request forgery vulnerability in the isSSRFSafeURL function that fails to extract embedded IPv4 addresses from NAT64, 6to4, and Teredo IPv6 transition address formats. Unauthenticated attackers can bypass SSRF protections via the LiveLinks proxy endpoint to reach internal services and cloud metadata endpoints by encoding private IPv4 targets in transition address formats.	7.5	More Details
CVE-2026-81688	openssl_encrypt versions before 1.4.9 store an unkeyed SHA-256 hash of the plaintext in the cleartext file header metadata. Attackers can read this hash without the password to confirm guessed plaintexts offline or fingerprint identical plaintexts across separately-encrypted files.	7.5	More Details
CVE-2026-81689	openssl_encrypt versions before 1.4.9 derive the remote-pepper wrap key using unsalted HKDF-SHA256 or bare SHA-256 of the password, allowing identical keys across all users and files. Attackers with access to wrapped pepper blobs can precompute a single dictionary table and perform fleet-wide offline password guessing at hardware speed to recover user passwords.	7.5	More Details
CVE-2026-30064	Improper input validation in the buildFilter function (processor/processor.go) of free5gc v4.0.1 allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2026-30063	An issue in the NF Discovery endpoint of free5gc v4.0.1 allows attackers to cause a Denial of Service (DoS) via a crafted snssais query.	7.5	More Details
CVE-2026-30062	An issue in the NGAP handler of free5gc v4.0.1 allows attackers to cause a Denial of Service (DoS) via a crafted NAS PDU.	7.5	More Details
CVE-2026-30060	An issue in free5gc v4.0.1 allows attackers to cause a Denial of Service (DoS) when parsing crafted SUCI data during UE registration.	7.5	More Details
CVE-2026-30059	An issue in the NAS decoder component of free5gc v4.0.1 allows attackers to cause a Denial of Service (DoS) via a crafted Registration Request message.	7.5	More Details
CVE-2026-30058	Improper Input Validation in the HTTPModifySubscription handler of free5gc v4.0.1 allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2026-30057	An issue in the CreateUEContext handler component of free5gc v4.1.0 allows attackers to cause a Denial of Service (DoS) via supplying a crafted request.	7.5	More Details
CVE-2026-30056	A NULL pointer dereference in the AMF NGAP Dispatcher component of free5gc v4.0.1 allows attackers to cause a Denial of Service (DoS) via supplying crafted NGAP messages during the initialization of a new RAN connection.	7.5	More Details
CVE-2026-30051	An issue in the CreateUEContextProcedure function (/v1/ue-contexts/{supi}) of free5gc v4.1.0 allows attackers to cause a Denial of Service (DoS) via supplying a crafted PUT request.	7.5	More Details
CVE-2026-30050	An issue in the ModifyAMFEventSubscriptionProcedure function (processor/event_exposure.go) of free5gc v4.1.0 allows attackers to cause a Denial of Service (DoS) via supplying a crafted PATCH request.	7.5	More Details
CVE-2026-30047	A reachable assertion vulnerability in the /nsmf-pdusession/v1/sm-contexts component of Open5GS v2.7.6 allows attackers to cause a Denial of Service (DoS) via supplying a crafted DELETE request.	7.5	More Details
CVE-2026-30046	A reachable assertion vulnerability in the NUDM-UECM interface of Open5GS v2.7.6 allows attackers to cause a Denial of Service (DoS) via supplying a crafted DELETE request.	7.5	More Details
CVE-2026-30045	An integer overflow in the /nnrf-disc/v1/nf-instances component of open5gs v2.7.6 allows attackers to cause a Denial of Service (DoS) via supplying a crafted HTTP/2 GET request.	7.5	More Details
CVE-2026-26459	ccoap 77f55c4b466e99327c24ace8a2913d3ba7e2ccd5 contains a vulnerability in the option parsing logic that causes a segmentation fault when processing malformed COAP messages with insufficient option data.	7.5	More Details
CVE-2026-26457	ccoap 77f55c4b466e99327c24ace8a2913d3ba7e2ccd5 contains a null pointer dereference vulnerability in the coap_dump_msg() function when processing COAP messages containing options with zero length.	7.5	More Details
CVE-2026-26456	A null pointer dereference vulnerability exists in the server-side session management logic of ccoap 77f55c4b466e99327c24ace8a2913d3ba7e2ccd5. The issue is caused by a race condition between the request dispatch thread and the session cleanup thread when accessing shared session list nodes without proper synchronization.	7.5	More Details
CVE-2026-26453	ccoap 77f55c4b466e99327c24ace8a2913d3ba7e2ccd5 contains a null pointer dereference vulnerability in the coap_server_handle_session() function when processing COAP messages containing URI_PATH options with NULL data pointers. When the server searches for a URI_PATH option matching the string "separate", it directly calls strncmp() on option_list[i].data without checking if the pointer is NULL. This causes a segmentation fault when the option's data field is NULL.	7.5	More Details
	openssl_encrypt versions before 1.4.9 fail to validate server URLs in login and register_with_email functions,		

CVE-2026-81691	accepting unencrypted http:// URLs and unconfigured hosts. Attackers on the network path can intercept cleartext credentials including client_id, passwords, and JWTs to achieve full keyserver account takeover.	7.5	More Details
CVE-2026-81692	openssl_encrypt (pip: openssl-encrypt) versions 1.4.8 and earlier fail to validate the 36-bit STREAMINFO total_samples field of FLAC files before using it to size an allocation (np.random.randint(size=(total_samples, channels))). A ~50-byte crafted FLAC file declaring ~100 million samples causes a multi-gigabyte memory allocation, leading to out-of-memory denial of service during 'decrypt --stego-extract'. The issue is fixed in 1.4.9; both the 1.4.x and 1.5.x lines are affected.	7.5	More Details
CVE-2026-81693	openssl_encrypt before 1.4.9 fails to validate the total field from QR JSON payloads before materializing ranges. Attackers can supply crafted QR images with extremely large total values to trigger unbounded memory allocation and cause denial of service through out-of-memory conditions.	7.5	More Details
CVE-2026-38348	An integer overflow in the libswscale/utils.c component of FFmpeg N-122528-gdd2976b9e1 allows attackers to cause a Denial of Service (DoS) via supplying a crafted image file.	7.5	More Details
CVE-2026-80637	In the Linux kernel, the following vulnerability has been resolved: netfilter: synproxy: fix unaligned memory access in timestamp adjustment Use get_unaligned_be32() and put_unaligned_be32() to safely read and write the timestamp fields. This prevents performance degradation due to unaligned memory access or even a crash on strict alignment architectures. This follows the implementation of timestamp parsing in the networking stack at tcp_parse_options() and synproxy_parse_options().	7.5	More Details
CVE-2026-80631	In the Linux kernel, the following vulnerability has been resolved: btrfs: lzo: reject compressed segment that overflows the compressed input lzo_decompress_bio() validates each on-disk segment length seg_len only against the workspace cbuf size, not against the compressed input size (compressed_len, the total folio bytes of the bio). A crafted extent can carry a segment whose seg_len passes the cbuf check but runs past the end of the bio, so copy_compressed_segment() walks off the last folio: get_current_folio() then returns the NULL folio from bio_next_folio(), and with CONFIG_BTRFS_ASSERT disabled (default) folio_size(NULL) faults. BUG: KASAN: null-ptr-deref in lzo_decompress_bio (fs/btrfs/lzo.c:383) Read of size 8 at addr 0000000000000000 by task kworker/u8:1/29 Workqueue: btrfs-endio simple_end_io_work kasan_report (mm/kasan/report.c:590) lzo_decompress_bio (fs/btrfs/lzo.c:383) end_bbio_compressed_read (fs/btrfs/compression.c:1065) btrfs_bio_end_io (fs/btrfs/bio.c:135) btrfs_check_read_bio (fs/btrfs/bio.c:180 fs/btrfs/bio.c:285) simple_end_io_work process_one_work worker_thread Reject any segment whose payload would extend beyond compressed_len before copying it, treating it as corruption like the other on-disk validation failures in this function.	7.5	More Details
CVE-2026-80614	In the Linux kernel, the following vulnerability has been resolved: net: emac: Fix NULL pointer dereference in emac_probe Move devm_request_irq() after devm_platform_ioremap_resource() so that dev->emacp is mapped before the interrupt handler can fire. An early interrupt hitting emac_irq() would dereference the NULL dev->emacp and crash. Also remove redundant error message. devm_platform_ioremap_resource() already returns an error message with dev_err_probe().	7.5	More Details
CVE-2026-5097	The wpForo Forum plugin for WordPress is vulnerable to SQL Injection via the 'referer' parameter in all versions up to, and including, 2.4.17. This is due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details
CVE-2026-19084	The shared-files-pro WordPress plugin before 1.7.70 does not validate the file path supplied when creating a featured image, allowing unauthenticated attackers to read arbitrary files from the server and republish their contents at a public URL.	7.5	More Details
CVE-2026-18983	The One User Avatar | User Profile Picture plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 2.5.4 via the wpua_action_process_option_update function. This is due to insufficient file type validation in wp_handle_upload() called without a MIME allow-list, with post-write validation relying on the attacker-controlled client-supplied Content-Type header rather than a server-derived type, and no cleanup of files that fail the check. This makes it possible for authenticated attackers, with subscriber-level access and above, to upload files that may be executable, which makes remote code execution possible. in order to exploit this vulnerability an admin has to give subscribers permission to upload avatars. While PHP files and svg files are rejected, dxfp files are accepted.	7.5	More Details
CVE-2026-76945	The affected Ebyte device relies on client-managed authentication tokens without sufficient server-side validation. An attacker may replay or manipulate authentication tokens to gain unauthorized access to administrative functionality.	7.5	More Details
CVE-2026-76940	The affected Ebyte device does not restrict repeated authentication attempts through rate limiting or account lockout mechanisms. This could allow an attacker to perform automated authentication attacks against deployments that rely on password based authentication.	7.5	More Details
CVE-2026-75813	Certain configuration endpoints may lack proper server-side authorization checks, allowing unauthorized users to access or modify sensitive device settings. This could result in full compromise of device functionality.	7.5	More Details
	A path traversal vulnerability exists in the built-in preview/development web server of Lektor <3.3.14 on		

CVE-2026-75418	Windows. An attacker with network access to the server can send a crafted HTTP request containing path traversal sequences to read arbitrary files accessible to the process, disclosing sensitive information such as system files and deployment configuration files containing credentials.	7.5	More Details
CVE-2026-73809	A cleartext transmission of sensitive information vulnerability exists in certain Ebyte gateway products. The web management interface does not adequately protect sensitive communications using transport-layer encryption. An attacker with access to network traffic could intercept authentication or session-related information transmitted between a user and the affected device. Successful exploitation could result in disclosure of sensitive information and unauthorized access to device management functionality.	7.5	More Details
CVE-2026-33605	An unauthenticated attacker can crash the ManageSieve login process by sending a small malformed command before authenticating. If running in high-security mode (default for community releases), only the attacker's own connection is terminated. If running in high-performance mode (default for Pro releases), all connections handled by the same managesieve-login process are terminated. Repeating the attack can cause denial of service for Sieve script management. Restrict network access to the ManageSieve service to trusted clients. Update to non-vulnerable version. No publicly available exploits are known.	7.5	More Details
CVE-2026-38350	An integer overflow in the target_sws_fuzzer() function (libswscale/output.c) of FFmpeg N-122528-gdd2976b9e1 allows attackers to cause a Denial of Service (DoS) via supplying a crafted input.	7.5	More Details
CVE-2026-38349	An integer overflow in the hScale16To19_c() function (libswscale/output.c) of FFmpeg N-122528-gdd2976b9e1 allows attackers to cause a Denial of Service (DoS) via supplying a crafted image file.	7.5	More Details
CVE-2026-38347	A heap overflow in the ff_sws_alphablendaway function (libswscale/alphablend.c) of FFmpeg git-master commit 722a217 allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2026-81698	openssl_encrypt versions before 1.4.9 contain a shell injection vulnerability in the info command's reconstructed CLI block that interpolates untrusted metadata fields without quoting. Attackers can craft metadata values like pepper_name containing shell commands that execute when users copy the printed CLI block into a shell.	7.5	More Details
CVE-2026-38346	An integer overflow in the yuv2planeX_8_c() function (libswscale/output.c) of FFmpeg N-122528-gdd2976b9e1 allows attackers to cause a Denial of Service (DoS) via supplying a crafted video file.	7.5	More Details
CVE-2026-38344	A NULL pointer dereference in the get_min_buffer_size function (/libswscale/slice.c) of FFmpeg N-122528-gdd2976b9e1 allows attackers to cause a Denial of Service (DoS) via supplying a crafted video file.	7.5	More Details
CVE-2026-77438	Trilium is an open-source hierarchical note-taking application. In versions up to and including 0.103.0, the public share-search endpoint does not enforce the per-note shareCredentials and shareHiddenFromTree controls, allowing an unauthenticated visitor to read the titles, tree paths, and content of protected shared notes. The endpoint authorizes only the ancestor note supplied in the request and then runs a full-text search across the entire published subtree, returning each matching note's title, share identifier, and hierarchical path without re-checking whether that individual note requires a share password or is hidden from the navigation tree. Because the search matches note content, an attacker can enumerate protected notes and use the endpoint as a boolean oracle that confirms arbitrary substrings, recovering the full contents of notes that should be gated behind a password. This issue is fixed in version 0.104.0.	7.5	More Details
CVE-2026-76640	Unitree G1 EDU firmware through 1.5.2 contains multiple chained vulnerabilities in the BLE GATT server and WiFi provisioning stack that allow unauthenticated proximate attackers to achieve root code execution without pairing or credentials by exploiting an unquoted heredoc variable in the WiFi provisioning script and a buffer overflow in the SSID chunk accumulator. Attackers can send crafted BLE writes to overflow a fixed BSS buffer across BLE connections, corrupting an adjacent mainloop function pointer dispatch entry that is subsequently invoked by the cleanup path passing attacker-controlled data to system() as uid 0.	7.5	More Details
CVE-2026-59289	Spring for GraphQL's Spring Data pagination support resolves arguments of a scrollable query and forwards the client-supplied values to the underlying repository. An attacker can forge a malicious query for a Connection field that can exhaust application memory or place significant, prolonged load on the underlying datastore, resulting in a Denial of Service. Spring for GraphQL 2.0.0 - 2.0.4 Spring for GraphQL 1.4.0 - 1.4.6 Spring for GraphQL 1.2.0 - 1.3.9	7.5	More Details
CVE-2026-59282	Spring Framework applications that use Spring's data binding infrastructure to apply user-supplied property paths onto a target object may be vulnerable to a Denial of Service (DoS) attack. Spring Framework 7.0.0 - 7.0.8 Spring Framework 6.2.0 - 6.2.19 Spring Framework 6.1.0 - 6.1.28 Spring Framework 6.0.0 - 6.0.30 Spring Framework 5.3.0 - 5.3.49 Spring Framework 5.2.25.RELEASE and earlier	7.5	More Details
CVE-2026-37198	An integer overflow in the SMF component of Open5GS v2.7.6 allows attackers to cause a Denial of Service (DoS) via supplying a crafted GTP packet.	7.5	More Details
CVE-2026-37012	A vulnerability in pentestgpt/core/langfuse.py in PentestGPT 1.0.0 allows remote attackers to disclose sensitive user telemetry data via hardcoded API credentials.	7.5	More Details
CVE-2026-81722	nltk PorterStemmer in versions <= 3.10.2 (fixed in 3.10.3) contains an inefficient-algorithmic-complexity denial of service in PorterStemmer.stem(). The _is_consonant() helper walks backward over the entire run of trailing 'y' characters on every call, and _measure() invokes it for each stem position, causing O(n^2) behavior. A single ~20-50 KB untrusted token consisting of a long run of the letter 'y' followed by a	7.5	More Details

	matching suffix (e.g., 'ness') can pin a CPU core for seconds to minutes, causing availability impact.		
CVE-2026-81721	openssl_encrypt before 1.4.9 fails to validate KDF cost parameters in encrypted file metadata and keystore headers, allowing attackers to trigger unbounded memory allocation. Attackers can craft malicious encrypted files declaring arbitrarily large Argon2, scrypt, or balloon KDF parameters to exhaust system memory and crash the process without authentication.	7.5	More Details
CVE-2026-81718	openssl_encrypt versions before 1.4.9 use under-parameterized PBKDF2-HMAC-SHA256 with only 100,000 iterations to protect PQC keyfile private keys and 10,000 iterations for dual-encryption file-password verification. Attackers who obtain keyfiles or encrypted files can brute-force wrapping passwords offline using GPU or ASIC acceleration.	7.5	More Details
CVE-2026-81705	openssl-encrypt before 1.4.9 fails to redact the file password in its --debug argv dump when the password is supplied via bundled short-option spellings (e.g. -apHunter2) or abbreviated long-option spellings (e.g. --passw). The sanitizer only recognized exact option names, --option=value forms, and tokens starting with -p, so these spellings bypass the redaction chokepoint and the cleartext password is written to stderr. Anyone with access to that output (terminal scrollback, merged 2>&1 output, CI job logs, or the GUI's persistent debug log) can recover the password.	7.5	More Details
CVE-2026-81704	openssl_encrypt versions before 1.4.9 contain a weak key derivation vulnerability in the D-Bus CryptoService.EncryptFile handler that uses unstretched SHA-256 instead of Argon2id. Attackers can perform offline password guessing against encrypted files roughly six to seven orders of magnitude faster than documented protection by exploiting the missing key stretching and hash rounds.	7.5	More Details
CVE-2026-81699	openssl_encrypt versions before 1.4.9 fail to properly validate key derivation function costs in crafted files, allowing attackers to trigger unbounded memory and CPU exhaustion during pre-authentication processing. Attackers can supply malicious files with excessive KDF parameters to exhaust system resources and crash or wedge the process before password verification occurs.	7.5	More Details
CVE-2026-27852	An attacker that can send mail to a user can craft a message whose headers contain a very large number of email addresses or MIME parameters, which causes excessive memory usage when the message is later parsed. The message is still delivered, but reading it over IMAP can exhaust the memory limit of the process and terminate it, causing denial of service for the affected user. Update to non-vulnerable version. No publicly available exploits are known.	7.5	More Details
CVE-2026-55484	ALOS HTTP is a Linux-first Go web framework and application server built around a custom networking stack. Prior to 0.0.0-20260617230736-314b6783e196, core/utils.go::sanitizeRequestPath calls splitPathQuery on a request path beginning with a question mark and then performs the unchecked p[0] access without checking whether the resulting path is empty. An unauthenticated client can send a malformed request such as a question-mark-only path through h1_plain.go::ParseH1RequestHead, hpack.go::decodeSimpleGetPathHTTPSRequest, hpack.go::observeHeader, or h3_conn.go::handleRequestStream, causing an out-of-bounds panic before core.Recovery() middleware runs and terminating the server process. This issue is fixed in pseudo-version 0.0.0-20260617230736-314b6783e196.	7.5	More Details
CVE-2026-26452	ccoap 77f55c4b466e99327c24ace8a2913d3ba7e2ccd5 lcontains a vulnerability in the option parsing logic that causes a segmentation fault when processing COAP messages containing invalid option numbers.	7.5	More Details
CVE-2026-82268	Qwen-Agent through 0.0.34 contains a server-side request forgery vulnerability in the document parsing path that treats caller-supplied paths as URLs without scheme restriction or host validation. Attackers can reach the unauthenticated Gradio interface to make the server issue HTTP requests to arbitrary internal addresses including metadata services and read retrieved content through parsed document output.	7.5	More Details
CVE-2026-19271	Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') vulnerability in TÜBİTAK BİLGEM Software Technologies Research Institute Liderahenk allows LDAP Injection. This issue affects Liderahenk: from 3.4.0 before 3.5.5.	7.5	More Details
CVE-2026-17203	IBM Administration Runtime Expert for i 1R1M0 could allow a remote authenticated attacker to obtain sensitive information due to improper authentication enforcement.	7.5	More Details
CVE-2026-26446	Stomper 5e2741e is vulnerable to Denial of Service. When a broker sends data to a client whose TCP connection was already closed by the peer, the server process receives SIGPIPE and immediately terminates, resulting in a denial of service. Any unauthenticated client can trigger the crash by closing the socket at specific points.	7.5	More Details
CVE-2026-26447	Stomper 5e2741e is vulnerable to Use-After-Free. When a single client repeatedly issues SUBSCRIBE commands for the same destination over one connection and then closes that connection, the broker performs incorrect cleanup of its internal subscription structures. This results in a heap use-after-free during StompClient destruction, causing the broker process to crash. An unauthenticated client can exploit this to reliably trigger a denial of service.	7.5	More Details
CVE-2026-26449	In Stomper 5e2741e when a client sends a SEND frame missing the destination header field, the server triggers a null pointer dereference (or access to invalid memory) while processing the frame, causing the process to crash.	7.5	More Details

CVE-2026-46369	Nimiq is a Rust implementation of the Nimiq Proof-of-Stake protocol based on the Albatross consensus algorithm. Through 1.5.0, the validity store uses a strict lower-bound comparison that expires a stored transaction too early relative to Transaction::is_valid_at, allowing a remote attacker to replay the same signed transaction during a blocks_per_batch minus one block window and cause the sender and recipient balances to be updated twice. This issue is fixed in version 1.5.1.	7.5	More Details
CVE-2026-15990	The Formidable Charts plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 2.0.1 via the 'frm_graph' parameter. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information. Successful exploitation requires Formidable Forms Lite, Formidable Forms Pro, and Formidable Charts to be active and requires the wp-content/uploads/frm-charts/ directory to exist, normally after an image-format chart is rendered.	7.5	More Details
CVE-2026-82288	Stable Diffusion WebUI through 1.10.1 contains a credential disclosure vulnerability in the /sdapi/v1/cmd-flags endpoint that returns parsed command-line arguments including gradio_auth and api_auth values in cleartext. Unauthenticated attackers can access this endpoint to retrieve configured usernames and passwords, then use them to authenticate to the interface and access the application.	7.5	More Details
CVE-2026-80205	NLTK versions before 3.10.0 contain a regular expression denial of service vulnerability in Text.findall() and TokenSearcher.findall() methods that accept user-supplied regular expressions without validation or timeout. Attackers can supply crafted regex patterns that cause catastrophic backtracking, resulting in indefinite CPU saturation and denial of service to all users of the Python process.	7.5	More Details
CVE-2026-80347	mcp-fetch checks a fetch target against its SSRF guard without removing the brackets that surround an IPv6 literal. isSafeUrl reads the hostname from the parsed URL, which for a literal such as http://[::1]/ yields the bracketed string, and then tests it with net.isIP. That call returns zero for a bracketed value, so the branch holding the private-address checks is skipped entirely. The guard falls back to resolving the hostname, the bracketed string is not a resolvable name, no addresses are returned, and the target is reported safe. The HTTP client then strips the brackets and connects. Because the address may be given in IPv4-mapped form, the same path reaches any IPv4 target the loopback and private checks were meant to exclude, including link-local metadata endpoints. isPrivateIPv6 also has no case for the ::ffff: prefix, so the mapped form would still pass even if the brackets were removed. The fetch target is supplied as a tool argument, so an attacker who can influence what the model requests can read internal responses back into the model context.	7.5	More Details
CVE-2026-68863	Dell PowerProtect One, versions 20.1.0.0 and below, contain a Stack-based Buffer Overflow vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Denial of service.	7.5	More Details
CVE-2026-82275	Qwen-Agent through 0.0.34 contains a path traversal vulnerability in the document parser that fails to restrict file access to intended directories. Attackers can supply absolute file paths to the unauthenticated Gradio interface to read arbitrary files accessible by the server process.	7.5	More Details
CVE-2026-82270	Portkey AI Gateway through 1.15.2 contains a server-side request forgery vulnerability in the /v1/proxy/* route that lacks requestValidator middleware. Attackers can set the x-portkey-custom-host header to internal addresses and forward requests with Authorization headers to reach internal services and exfiltrate provider API keys.	7.5	More Details
CVE-2025-51675	An issue was discovered in openRISC OR1200 commit 83ac6b. An inaccurate update of program counter (PC) values when SPR changes can lead to a Denial of Service (DoS).	7.5	More Details
CVE-2026-51659	Incorrect access control in the getUrlFilterRules function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain DMZ configuration information via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	7.5	More Details
CVE-2025-61478	An issue in Vanderbilt Industries, Acre Security SPC5300.000 Main Board v.3.14.1 allows a physically proximate attacker to cause a denial of service via Spoofed SYN packets.	7.5	More Details
CVE-2025-61479	An issue in Vanderbilt Industries, Acre Security SPC5300.000 Main Board v.3.14.1 allows a physically proximate attacker to cause a denial of service via the SPC Connect Pro software accepts replayed application-layer payloads injected into an active TCP session.	7.5	More Details
CVE-2025-61480	An issue in Vanderbilt Industries, Acre Security SPC5300.000 Main Board v.3.14.1 allows a physically proximate attacker to cause a denial of service via spoofed TCP FIN packets without validating the sequence or acknowledgment numbers.	7.5	More Details
CVE-2026-75124	PLANET GS-4210-16P2S V3 firmware before 3.441b260626 contains a pre-authentication memory corruption vulnerability in the web management interface where the _readHttpParam function copies an oversized HTTP query string without guaranteeing NUL termination, allowing parse_query_string to process attacker-controlled data into a fixed-size stack buffer. An unauthenticated remote attacker can send an oversized GET request to dispatcher.cgi to cause denial of service of the web management interface and potentially trigger memory corruption.	7.5	More Details
CVE-2026-81624	Undertow is a flexible performant web server used in JBoss EAP and WildFly. A flaw was found in how Undertow handles WebSocket connections. Specifically, certain configuration limits like message buffer sizes and session timeouts cannot be adjusted and default to being unlimited. This allows a remote attacker to send large amounts of data or maintain connections indefinitely, potentially crashing the server by	7.5	More Details

	exhausting its memory or other resources.		
CVE-2026-16444	Improper neutralization of path traversal sequences in TeamViewer Desktop Clients prior Version 15.81.5 allows an authenticated remote session participant to write files to unintended locations on the local file system via file transfer or virtual file clipboard mechanisms. An attacker can leverage this behavior to achieve arbitrary file write and potentially execute code with the privileges of the affected user.	7.5	More Details
CVE-2026-82861	@hulumi/policies versions before 1.3.2 contain a parent spoof bypass vulnerability that allows attackers to submit spoofed SecureBucket parent evidence during policy evaluation. Attackers can bypass security policy checks by providing falsified evidence, causing the validator to miss unsafe bucket configurations.	7.5	More Details
CVE-2026-55584	phpSysInfo is a customizable PHP script that displays system information. Prior to 3.4.6, the PSI_ALLOWED access-control check in read_config.php trusts attacker-controlled X-Forwarded-For and Client-IP HTTP headers before REMOTE_ADDR. A remote unauthenticated attacker can supply an allowed address in one of these headers to impersonate a trusted client and access exposed hostname, kernel, CPU, memory, filesystem, and network-interface information. This issue is fixed in version 3.4.6.	7.5	More Details
CVE-2026-55552	Yamcs is a mission control framework. Prior to 5.11.13, Yamcs StaticFileHandler.locateFile resolves an unauthenticated request path without using Path.normalize and Path.toAbsolutePath to confirm that the absolute path remains within the configured staticRoots. A path containing traversal segments can escape the intended web root and return an arbitrary readable host file. The flaw is in yamcs-core/src/main/java/org/yamcs/http/StaticFileHandler.java and can disclose sensitive operating-system and application data. This issue is fixed in version 5.11.13, and the 5.12 line is fixed from version 5.12.0.	7.5	More Details
CVE-2026-75413	DocSys V2.02.80 is vulnerable to Any File Download. An attacker does not need to go through authentication to utilize the downloadDocEx.do interface and download any file via the parameter targetPath.	7.5	More Details
CVE-2026-75415	AntFlow V2.0.0 is vulnerable to Incorrect Access Control. JiMuMDCCommonsRequestLoggingFilter.java retrieves the userid from the request header as the core of the identity verification mechanism, allowing attackers to forge any user identity credential information, thereby causing sensitive information leakage.	7.5	More Details
CVE-2026-80527	In the Linux kernel, the following vulnerability has been resolved: ceph: fix hanging __ceph_get_caps() with stale mds_wanted A reader can hang forever in __ceph_get_caps() when the client no longer holds `FILE_RD`, but local cap state still says that the capability is already wanted (via `mds_wanted`). One way to trigger this is through MDS cap revocation. If another client performs a conflicting operation, the MDS can revoke `FILE_RD` from the reader; the next read then has to reacquire `FILE_RD`. If the cap update that should request `FILE_RD` never reaches the MDS after `cap->mds_wanted` was raised, the reader is left holding only non-file caps while local `mds_wanted` still includes the file read caps. In that state, try_get_cap_refs() sees `need <= mds_wanted` and returns 0, so __ceph_get_caps() just waits on `i_cap_wq`. If the cap update that was supposed to request `FILE_RD never reaches the MDS after `cap->mds_wanted was` raised, no further request is sent and the waiter can sleep indefinitely until unrelated cap traffic happens to wake it up. The ordering issue is that `cap->mds_wanted` is updated in __prep_cap() before the `CEPH_MSG_CLIENT_CAPS message` is actually queued for send. That makes one field serve two different meanings at once: what this client wants, and what the client believes the MDS already knows it wants. A proper fix would be to split those states and track whether a cap update is actually in flight or has been observed by the MDS. However, simply moving the `cap->mds_wanted assignment` later would not be sufficient: queueing the message in the messenger does not guarantee that the MDS processed that specific wanted set, and reconnect or message loss can still invalidate that assumption. Fixing that properly would require a larger rework of the cap state machine. To allow simpler backports to stable kernels, this patch implements a simpler workaround: - stop waiting forever in __ceph_get_caps(); after a bounded wait, fall back to the renew path - make ceph_renew_caps() issue a synchronous `OPEN` request whenever the inode still does not actually hold the wanted caps, instead of only calling ceph_check_caps() The extra issued-vs-wanted check in ceph_renew_caps() is necessary because the previous test only checked whether the inode still had any real caps at all. That is not enough after revocation: the client can still hold something like `pLs` and yet be missing `FILE_RD` completely. In that case, falling back to ceph_check_caps() is not sufficient, because it still trusts `cap->mds_wanted` and may resend nothing. By requiring `(issued & wanted) == wanted` before taking the asynchronous path, the code only uses ceph_check_caps() when the `wanted caps` are already actually issued. Otherwise, it sends the synchronous `OPEN` renew. This preserves the existing asynchronous fast path when the wanted caps are already issued, avoids changing cap-state semantics, and fixes the hang by guaranteeing that a stalled waiter eventually retries through a path that does not rely on the stale `mds_wanted` state. [idryomov: move CEPH_GET_CAPS_WAIT_TIMEOUT from libceph.h to mds_client.h, formatting]	7.5	More Details
CVE-2026-19873	HTML::FormFu versions through 2.08 for Perl allow resource exhaustion via an unbounded repeat count from the query string in Repeatable elements. When a Repeatable element has counter_name set, its process method reads the repeat count from the named query string parameter, checks only that it is a positive integer, and passes it to repeat, which deep-clones the element's child subtree once per iteration. Nothing caps the value, and no attribute lets an application impose a limit. The count is read on every request, before the form decides whether it was submitted, so a plain GET reaches the clone loop with no credentials, no session and no request body. Nesting multiplies: a Repeatable inside a Repeatable takes a counter at each level, so an outer and an inner value of 100 build 10,000 clones. Once the form is submitted, each cloned field's constraints scan the whole element tree in _find_field_value, so cost grows faster than linearly with the count. A single request exhausts memory and CPU. The latest release on CPAN is 2.07, from 2018.	7.5	More Details

	Version 2.08 exists only in the git repository.		
CVE-2026-18899	IBM Langflow OSS 1.0.0 through 1.11.1 could allow a remote attacker to read arbitrary files due to path traversal.	7.5	More Details
CVE-2026-51662	Incorrect access control in the getCloudSrvCheckStatus function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain cloud firmware check status information via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	7.5	More Details
CVE-2026-36851	Path traversal vulnerability in UnPoller 2.33.0 password field allows arbitrary file read and network exfiltration.	7.5	More Details
CVE-2026-77037	multer is a middleware for handling multipart/form-data in Node.js. In version 2.2.0, when a disk-backed upload is aborted or truncated before the write stream finishes, multer's disk storage engine removes the visible file but does not close the underlying write file descriptor, leaving a deleted but still open descriptor. A remote attacker able to reach an upload route using the built-in disk storage can send repeated aborted or malformed multipart uploads, each one leaking a file descriptor and retaining disk blocks until the process exits, which can exhaust resources and cause a denial of service. The issue is fixed in multer 2.3.0, which closes the destination write stream on abnormal source termination and defers cleanup until the stream has closed. Upgrade to multer 2.3.0 to remediate.	7.5	More Details
CVE-2026-80520	In the Linux kernel, the following vulnerability has been resolved: ovpn: fix NULL dereference when killing missing key ovpn_crypto_kill_key assumes both crypto slots are populated and dereferences each slot before checking it. That is not guaranteed: a peer can have only one installed key, and the kill path may be asked to remove a key that is not present. Read each slot once while holding the crypto state lock, check for NULL before looking at key_id, and only replace the slot that actually matches.	7.5	More Details
CVE-2026-82639	NextChat versions from 2.15.8 through 2.16.1 contain an improper URL validation vulnerability in the proxy endpoint that allows attackers to obtain the server's OpenAI API key. The x-base-url header is validated using substring matching instead of hostname parsing, allowing any URL containing 'api.openai.com' to pass validation and receive the server's credentials in the Authorization header.	7.5	More Details
CVE-2026-75807	The SAML Single Sign On – SSO Login plugin for WordPress is vulnerable to Authentication Bypass in versions up to, and including, 5.4.6. This is due to the mo_saml_login_validate() ACS handler persisting the X.509 certificate extracted from an incoming SAMLResponse into the mo_saml_required_certificate option before the signature-validation verdict is enforced, because mo_saml_find_certificate() returns false on a fingerprint mismatch rather than halting execution. This makes it possible for unauthenticated attackers to overwrite the plugin's stored IdP signing certificate with an attacker-controlled value, and subsequently forge SAML assertions for any WordPress account — including administrators — to obtain a fully privileged session. Note: The exploit requires the administrator to perform a repair after receiving the test_config_error_wpsamlerr004 error message during the test configuration.	7.5	More Details
CVE-2026-74750	In the Linux kernel, the following vulnerability has been resolved: ovpn: defer key slot crypto freeing to workqueue Key slots are released through a kref and the existing release path frees the AEAD transforms from an RCU callback. That is not safe for all crypto implementations: crypto_free_aead can sleep, for example when an async or hardware implementation has teardown work to complete. Use queue_rcu_work for key-slot release. This keeps the RCU grace period needed by lockless key-slot readers, but runs the actual crypto teardown from workqueue context where sleeping is allowed. Once the rcu_work callback runs, pre-existing RCU readers are gone, and the final kref put already proves that no transform user remains, so the worker can release the AEAD transforms and free the slot directly. The previous patch drains ovpn_wq during module exit, so queued key-slot teardown work cannot outlive module text.	7.5	More Details
CVE-2026-82472	Documenso before 2.13.0 accepts PDF file uploads on the /api/files/upload-pdf endpoint without requiring authentication, session tokens, or API credentials. Unauthenticated attackers can upload arbitrary PDF files indefinitely to exhaust storage resources or fill the database with unlinked document records.	7.5	More Details
CVE-2026-82453	rust-iot-platform through commit 5df942ab stores user passwords in cleartext without hashing in the user model. Attackers can read API responses from user retrieval and listing routes to obtain plaintext credentials for all accounts.	7.5	More Details
CVE-2026-74745	In the Linux kernel, the following vulnerability has been resolved: eth: bnxt: avoid deadlock when canceling IRQ affinity notifier Unregistering IRQ affinity notifiers waits for the callback synchronously. bnxt takes the netdev instance lock in the notifier (to restart the queue) and cancels the work under the same lock. This may obviously deadlock. Move the restart to the async service task. The queue restart isn't super time sensitive. Store the new TPH tag, schedule the task. Safely canceling the service task is already ironed out. In bnxt_request_irq() the order of registering notifier, affinity and initial TPH programming has to be inverted. I think it was racy previously since user may trigger an update as soon as notifier is installed. There's a small known gap - if pcie_tph_get_cpu_st() fails at init and the target tag is 0 we may miss programming the entry. This does not seem worth fixing, the code has skip-on-failure all over the place, anyway.	7.5	More Details
	In the Linux kernel, the following vulnerability has been resolved: veth: fix queue index used to wake the peer txq in veth_poll veth_poll() derives the index of the peer TX queue to wake from rq->xdp_rxq.queue_index. That field is only initialized by xdp_rxq_info_reg() in veth_enable_xdp_range(), which runs only when an XDP program is attached. On the plain GRO/NAPI path (veth_napi_enable_range())		

CVE-2026-74742	xdp_rxq_info_reg() is never called, so queue_index stays 0 for every queue, as priv->rq is zero-allocated. So in a multi-queue setup with GRO enabled and no XDP program attached, every NAPI instance looks at the peer's TX queue 0. If veth_xmit() stops peer TX queue 1 because the ptr_ring is full (NETDEV_TX_BUSY), nothing ever wakes it again: the poller draining queue 1 wakes queue 0 instead. veth implements no ndo_tx_timeout, so the netdev watchdog does not kick in either, and the queue stays stopped indefinitely. Derive the index from the position of the rq within priv->rq instead, which is correct regardless of whether XDP was ever enabled. Scripts to reproduce the stall are available at https://github.com/netoptimizer/veth-backpressure-performance-testing	7.5	More Details
CVE-2026-77007	The HEL Online Classroom: AI-powered Online Classrooms WordPress plugin through 1.0.3 does not perform any authorisation check on one of its REST API routes, allowing unauthenticated users to retrieve its stored settings, including the shared secret used to sign API requests to the connected BigBlueButton server.	7.5	More Details
CVE-2026-80588	In the Linux kernel, the following vulnerability has been resolved: mptcp: reclaim forward-allocated memory on RX path errors After commit 9db5b3cec4ec ("mptcp: borrow forward memory from subflow"), errors in the receive path prior to queueing skbs into the receive queue do not trigger forward-allocated memory reclaiming. Prevent forward memory from growing unboundedly in pathological drop scenarios by explicitly reclaiming memory when skbs are dropped.	7.5	More Details
CVE-2026-76586	The Appointment Booking Calendar Plugin and Scheduling Plugin WordPress plugin before 1.6.3 does not verify the amount actually paid against the server-side price staged for a booking when confirming an online payment, allowing unauthenticated users to have a paid appointment approved for a fraction of its price.	7.5	More Details
CVE-2026-55841	Graylog is a free and open log management platform. Prior to Graylog Server versions 6.3.12, 7.0.7, and 7.1.2 and Graylog Forwarder version 7.3, the FortiGate key-value syslog parser in graylog2-server/src/main/java/org/graylog2/inputs/codecs/GLFortiGateSyslogEvent.java and graylog2-server/src/main/java/org/graylog2/inputs/codecs/SyslogCodec.java mishandles field-like text inside quoted values. GLFortiGateSyslogEvent.getFields() uses KV_PATTERN and QUOTED_KV_PATTERN, while SyslogCodec.parse() invokes the FortiGateSyslogEvent parser; crafted values containing = or backslash-escaped quotes can cause embedded keys such as srcip, dstip, date, time, and tz to remove or overwrite original top-level fields or produce an invalid message that Graylog discards. An unauthenticated network sender who can submit syslog messages can therefore manipulate security-log fields or evade logging to obscure malicious activity. This issue is fixed in Graylog Server versions 6.3.12, 7.0.7, and 7.1.2 and Graylog Forwarder version 7.3.	7.5	More Details
CVE-2026-74741	In the Linux kernel, the following vulnerability has been resolved: net: ngbe: fix NULL pointer dereference in non-MSI-X interrupt enabling In non-MSI-X mode (such as legacy INTx or single MSI), wx->msix_entry is not allocated or initialized. Calling NGBE_INTR_MISC(wx) dereferences wx->msix_entry->entry, leading to a NULL pointer dereference crash. This issue was introduced by fixing the IRQ vector when the number of VFs is 7. Fix the issue by explicitly checking `pdev->msix_enabled` to determine the correct vector index. Additionally, as a side fix, set the interrupt mask to BIT(0) for the non-MSI-X fallback. In MSI/INTx mode, the MISC and queue interrupts share vector 0, and the WX_PX_MISC_IVAR register is only valid in the MSI-X case. Thus, BIT(0) is the correct mask for the miscellaneous cause when MSI-X is disabled.	7.5	More Details
CVE-2026-55784	free5GC is an open-source implementation of the 5G core network. In version 1.4.4 and earlier, the AUSF component stores per-subscriber authentication state in a global sync.Map named AUSFContext.UePool in internal/context/context.go, keyed only by SUPI. Every request handled by internal/sbi/processor/ue_authentication.go creates an AusfUeContext, and AddAusfUeContextToPool executes ausfContext.UePool.Store(ausfUeContext.Supi, ausfUeContext), unconditionally replacing the active context for that SUPI. An attacker with access to the AUSF SBI/N12 interface can send concurrent POST /nausf-auth/v1/ue-authentications requests for the same target SUPI, causing all attempts to share one logical authentication context URL while K_aut, XRES, and EapID are repeatedly overwritten. A valid EAP-AKA' response for an earlier challenge is then checked against the latest context, causing AT_MAC verification to fail and denying authentication to the selected subscriber while the request flood continues. No fixed version is available as of this review.	7.5	More Details
CVE-2026-82333	multer is a middleware for handling multipart/form-data in Node.js. A small multipart request with two specially crafted text field names can make multer's field parser synchronously iterate a maximum-length sparse array, blocking the event loop so the process cannot handle other requests. A large numeric array index in the first field allocates a maximum-length sparse array, and a second field with a non-numeric key then triggers a full-length iteration inside the append-field dependency. All versions before 2.3.0 are affected, and this is a remotely triggerable denial of service. multer 2.3.0 adds an opt-in fieldArrayIndexLimit option that rejects oversized array indexes. Upgrade to multer 2.3.0 and set limits.fieldArrayIndexLimit to the largest array index your application needs to remediate.	7.5	More Details
CVE-2026-82644	WWBN AVideo (current e01e41ecc and earlier) contains a brute-force rate limiting bypass in enforceRateLimit(), which protects login.json.php and 13 other endpoints. The function stores its attempt counter via a cache layer (ObjectYPT::setCacheGlobal) that silently discards writes for any client identified as a bot by isBot(). Because isBot() treats a missing User-Agent header as a bot by default — and also matches common bot identifiers such as 'curl', 'bot', 'crawler', and 'spider' — the counter never increments for such clients, so the rate limit never fires. An unauthenticated attacker can therefore submit unlimited login attempts (e.g., by omitting the User-Agent header or using curl's default User-Agent), enabling unrestricted password-guessing attacks.	7.5	More Details

CVE-2026-81520	A network-reachable client that has not yet authenticated can hold a MongoDB Connector for BI authentication session open indefinitely by beginning a SASL-based login exchange and then declining to complete it. Because the negotiation loop had no overall time bound and the read from the client had no deadline, each such session retains a worker, a client connection slot, and its associated backend database connections until the process is restarted. Repeated use of this behavior can consume the configured connection capacity and prevent legitimate users from establishing new sessions.	7.5	More Details
CVE-2026-81518	When mongosqld is configured with a client certificate authority file, the listener requests a client certificate during the TLS handshake but does not require one, so a client that presents no certificate is still accepted. In deployments that rely on client certificates as the sole means of identifying users, a remote party with network access to the listener can therefore establish a session and read the MongoDB data exposed through the connector.	7.5	More Details
CVE-2026-42391	An unauthenticated attacker can send an IMAP ID command with a very large number of parameters before logging in, which causes memory and CPU usage to grow disproportionately. The login process can be terminated by the out-of-memory handling, which also terminates all other connections handled by the same process. This can cause degradation or denial of service for IMAP logins. Limit the number of connections handled by a single imap-login process. This has a performance impact though. Update to non-vulnerable version. No publicly available exploits are known.	7.5	More Details
CVE-2026-82655	Admidio before 5.0.12 contains a blind SQL injection vulnerability in the relation_type_list parameter of lists_show.php that allows unauthenticated attackers to execute arbitrary SQL queries. Attackers can bypass authentication by providing a dummy UUID in role_list and inject SQL through relation_type_list to extract database contents including password hashes and user credentials.	7.5	More Details
CVE-2026-81517	An unauthenticated party able to reach the port of a MongoDB Connector for BI (mongosqld) instance may generate enough routine connection log activity to exhaust the storage backing the configured log path. When a log write or log rotation operation subsequently fails, the resulting error is not handled and the shared mongosqld process ends, ending service for all connected SQL clients. The process continues to end on startup until an operator restores available storage, and the diagnostic message explaining the condition is not recorded.	7.5	More Details
CVE-2026-82657	Admidio before 5.0.12 fails to enforce login-only module restrictions in RSS feed endpoints for forum and announcements modules. Unauthenticated attackers can retrieve forum topics and announcements by sending GET requests to rss/forum.php or rss/announcements.php, disclosing titles, full post text, author names, and timestamps.	7.5	More Details
CVE-2026-56718	AJCloud AJY IPC firmware prior to version 01.10715.11.37 contains a path traversal vulnerability in the jdbhttpd web service that allows unauthenticated remote attackers to read arbitrary files with root privileges by supplying path traversal sequences in the HTTP request URI. Attackers can send crafted HTTP requests to port 80 without authentication to access sensitive files including cleartext RTSP credentials, Wi-Fi SSID and pre-shared key, device serial number, and cloud binding parameters.	7.5	More Details
CVE-2026-77078	multer is a middleware for handling multipart/form-data in Node.js. A small multipart request containing two specially crafted text field names can cause an uncaught RangeError (Invalid array length) that terminates the Node.js process. The first field uses a very large numeric array index to allocate a maximum-length sparse array, and a second field then pushes past that length, which throws inside the append-field dependency and is not caught by multer. All versions before 2.3.0 are affected, and the issue is a remotely triggerable denial of service. The issue is fixed in multer 2.3.0. Upgrade to multer 2.3.0 to remediate.	7.5	More Details
CVE-2025-61162	Incorrect access control in Cohere North AI v1.1.5 allows attackers to arbitrarily overwrite user info via a crafted request to the /api/internal/v1/users/{{USER_ID}} endpoint	7.5	More Details
CVE-2025-61164	Cohere North AI v1.1.5 was discovered to contain an information leak via the WebSocket Endpoint.	7.5	More Details
CVE-2026-73108	RustDesk versions before 1.4.7 contain an uncontrolled speculative memory allocation vulnerability in BytesCodec. Before authentication, the decoder trusts the payload length encoded in a four-byte frame header and reserves that amount before receiving the payload. A crafted header can request up to 1,073,741,823 bytes of capacity, allowing unauthenticated attackers to use concurrent TCP connections to cause memory exhaustion and denial of service. The fix caps header-triggered speculative preallocation at 256 KiB.	7.5	More Details
CVE-2026-54788	dd-trace-rs provides Datadog application performance monitoring for Rust. From 0.1.0 until 0.3.3, datadog-opentelemetry/src/propagation/tracecontext.rs parses the W3C tracestate header and collects every semicolon-separated key and value pair in the Datadog dd=... vendor entry into a HashMap without enforcing a pair count or entry size limit. Because tracecontext extraction is enabled by default, a remote unauthenticated attacker can send an arbitrarily large dd=... entry and force excessive CPU and memory consumption for each request, causing denial of service in an instrumented network service. This vulnerability is fixed in 0.3.3.	7.5	More Details
	MariaDB Connector/Node.js is used to connect applications developed on Node.js to MariaDB and MySQL databases. Prior to versions 3.3.3, 3.4.6, and 3.5.3, when ssl is enabled without a pinned CA or server certificate, MariaDB Connector/Node.js sends credentials before completing certificate fingerprint validation.		

CVE-2026-55215	In lib/cmd/handshake/auth/handshake.js, a server that selects mysql_clear_password as the initial authentication plugin can receive the password before the post-TLS identity check. In lib/cmd/handshake/authentication.js, an authentication switch can evaluate the previous plugin instead of the requested target plugin, allowing mysql_clear_password to send the credential first. An active man-in-the-middle can present a self-signed certificate, capture the database password, and use it to authenticate directly even though the connector later rejects the server and closes the connection. This issue is fixed in versions 3.3.3, 3.4.6, and 3.5.3.	7.5	More Details
CVE-2026-51658	Incorrect access control in the getDmzCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain DMZ configuration information via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	7.5	More Details
CVE-2026-79407	A path traversal vulnerability in the SPO extension of MetaGPT 0.8.1 allows an attacker to read arbitrary files via the FILE_NAME value used by set_file_name() and load_meta_data() in metagpt/ext/spo/utils/load.py. The vulnerable code joins the attacker-controlled FILE_NAME value with the settings directory and opens the resulting path without validating that the resolved path remains within the intended directory.	7.5	More Details
CVE-2026-51650	Incorrect access control in the getRemoteCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain remote-management enablement and port information via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	7.5	More Details
CVE-2026-74928	The Project Manager WordPress plugin before 4.0.7 does not have any authorisation check on its import routes, allowing unauthenticated users to create WordPress accounts with a password the attacker already knows, bypassing the site's own registration setting.	7.5	More Details
CVE-2026-51716	Incorrect access control in the delPortForwardRules function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to delete port-forwarding rules via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	7.5	More Details
CVE-2026-81285	Unauthenticated Denial of Service Attack in Smush Image Compression and Optimization <= 4.2.0 versions.	7.5	More Details
CVE-2026-51719	Incorrect access control in the delUrlFilterRules function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to remove URL filtering rules via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	7.5	More Details
CVE-2026-75133	Keep Backup Daily plugin for WordPress before 2.1.4 contains a sensitive information exposure vulnerability that allows unauthenticated attackers to trigger a full MySQL database dump by accessing the publicly exposed `kbd_cron_process` parameter without authentication. Attackers can predict the partially predictable dump filename based on the database name, a limited random range, and the current Unix timestamp to download the generated backup from the publicly accessible uploads directory.	7.5	More Details
CVE-2026-17615	A flaw was found in RESTEasy's SourceProvider. This vulnerability allows an unauthenticated attacker to perform an unauthenticated remote file read. By sending a specially crafted XML body with a DOCTYPE declaration referencing external entities to an endpoint that accepts application/xml and returns Source or StreamSource, the server can be tricked into resolving the entity and including sensitive file contents in the HTTP response. This is due to the SourceProvider.writeTo() method creating a SAXParser without disabling external entity resolution, leading to an XML External Entity (XXE) vulnerability.	7.5	More Details
CVE-2026-51735	Incorrect access control in the showSyslog function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to retrieve recent system logs via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	7.5	More Details
CVE-2026-56854	The source-address critical option in the Permissions returned by an authentication callback was only enforced for the PublicKeyCallback and VerifiedPublicKeyCallback paths, extending the fix for CVE-2026-46595. Permissions returned by the PasswordCallback, KeyboardInteractiveCallback, NoClientAuthCallback, and GSSAPIWithMICConfig.AllowLogin callbacks were not validated against the client's remote address, so a source-address restriction set by those callbacks was silently ignored. The check is now applied to the Permissions returned by any authentication callback.	7.5	More Details
CVE-2026-54598	Wallos is an open-source, self-hostable personal subscription tracker. Prior to version 4.9.4, endpoints/db/migrate.php executes database schema migrations when called over HTTP with zero authentication. Any unauthenticated attacker can trigger pending migration files against the live SQLite database. This issue has been patched in version 4.9.4.	7.5	More Details
CVE-2026-38638	An issue in the with_argv function (/unistd/mod.rs) of relibc commit 61f42d allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2026-38636	An issue in the seekdir() function (/dirent/mod.rs) of relibc commit 61f42d allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2026-37736	An issue in the JsonSanitizer.sanitize() component of OWASP json-sanitizer v1.2.3 allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
	vLLM up to and including 0.17.0 allows remote attackers to cause a Denial of Service via memory		

CVE-2026-37237	exhaustion. The AsyncMediaIO.fetch_audio and AsyncMediaIO.fetch_image functions in multimodal/inputs.py fetch user-supplied media URLs using aiohttp and call r.read() without enforcing a maximum response size, allowing an attacker to exhaust server memory by providing a URL to an arbitrarily large file.	7.5	More Details
CVE-2026-47852	A local attacker on a multi-user host can pre-create the deterministic cache path and plant a malicious ONNX model file. Spring AI 2.0.0 Spring AI 1.1.0 - 1.1.8 Spring AI 1.0.0 - 1.0.9	7.5	More Details
CVE-2026-82261	SvelteKit (@sveltejs/kit) versions >=2.49.0 and <=2.52.1 with experimental remote functions and form enabled contain a CPU exhaustion vulnerability in form deserialization. An attacker can send malformed form data to cause the server to become unresponsive while processing the request, resulting in denial of service. Fixed in 2.52.2.	7.5	More Details
CVE-2026-82260	SvelteKit (@sveltejs/kit) versions >=2.49.0 and <=2.52.1 with experimental remote functions (experimental.remoteFunctions) and form enabled contain a memory exhaustion vulnerability in remote form deserialization. Malformed form data can cause excessive memory allocation, crashing the server process and resulting in denial of service. Fixed in 2.52.2.	7.5	More Details
CVE-2026-82259	SvelteKit versions from 2.49.0 through 2.53.2 (fixed in 2.53.3) contain a deserialization expansion issue in the experimental form remote function. When an application enables experimental.remoteFunctions and uses the form function to process the files array without validating files.length or individual file sizes, an attacker can submit relatively small inputs that expand into very large file arrays, leading to expensive processing and denial of service.	7.5	More Details
CVE-2026-82254	gitoxide before 0.69.0 contains unchecked array indexing in delta application and uncapped allocation from attacker-controlled size headers in gix-pack. Attackers can send crafted pack data during clone or fetch operations to trigger panics or out-of-memory process kills.	7.5	More Details
CVE-2026-82253	gitoxide (Rust crates gix <= 0.72.0 and gix-validate <= 0.10.0) contains a path traversal vulnerability. The submodule name validation function in gix-validate only checks the first occurrence of '..' via name.find(b".."), allowing crafted names such as 'a..b/../../../.git/' to bypass the check; additionally this validation is never invoked in production code paths. Combined with a trust inheritance flaw in Submodule::open(), where the parent repository's git_dir_trust (Trust::Full) is cloned and the ownership verification is skipped, an attacker can craft a malicious .gitmodules file so that a victim tool built on gitoxide reads arbitrary git repository configuration (including embedded credentials) with full trust, bypassing safe-directory protections. Fixed in gix 0.82.0 and gix-validate 0.11.1.	7.5	More Details
CVE-2026-82252	gitoxide before 0.52.1 follows symlinks when reading the worktree .gitmodules file, allowing attackers to inject out-of-repository bytes into submodule metadata. Attackers can create a malicious repository with a symlinked .gitmodules pointing outside the repository tree, causing gitoxide to parse arbitrary external files as submodule configuration and expose attacker-controlled name, path, and url values.	7.5	More Details
CVE-2026-82251	gitoxide before 0.52.1 fails to validate submodule names from .gitmodules configuration, allowing path traversal when deriving submodule git directories. Attackers can craft malicious submodule names with traversal segments to redirect state() and open() functions to repositories outside .git/modules, causing repository confusion and inspection of attacker-controlled repositories.	7.5	More Details
CVE-2026-82247	gitoxide's gix-url crate (<= 0.32.0, fixed in 0.37.1) uses a hand-rolled URL parser that does not treat '?' or '#' as terminating the authority component, contrary to RFC 3986. As a consequence, gix-transport's HTTP redirect identity guard (can_reuse_identity) compares the wrong host and fails open. An attacker controlling a redirect response can craft a Location header of the form <attacker-authority>?@<original-authority> so that gitoxide sends the caller's HTTP Basic Authorization credentials to an unintended host. gix-transport is affected in versions <= 0.49.0 (fixed in 0.58.1).	7.5	More Details
CVE-2026-80198	Kimai versions before 2.56.0 fail to restrict the config() Twig function in sandboxed invoice and export templates, allowing administrators to access arbitrary configuration keys. Attackers with admin privileges can upload malicious templates to exfiltrate server-wide secrets including LDAP bind passwords and SAML private keys into invoice or export documents accessible to lower-privileged users.	7.5	More Details
CVE-2026-80196	Kimai before 2.58.0 contains an authentication bypass vulnerability where password reset links remain valid after password changes because the LoginLink signature covers only the user id, not the password hash. Attackers who intercept or cache a password reset link can use it up to 2 additional times within a 1-hour window to log in as the user even after the legitimate user has changed their password.	7.5	More Details
CVE-2026-80191	GROWI applies its page-viewer permission check to attachment requests only when the request carries an authenticated user. retrieveAttachmentFromIdParam in apps/app/src/server/routes/attachment/get.ts guards the check with a condition requiring the user to be non-null, so a request that carries no session skips the check entirely and the handler returns the file. The routes reached this way, /attachment/:id and /download/:id, take the attachment identifier from the path, so an unauthenticated caller who has an attachment identifier receives the file regardless of whether the page owning it is private and regardless of whether that caller would be permitted to view the page. Identifiers can be retained by a user whose access was later removed, or recovered from anywhere the identifier was previously exposed. Version 8.0.2 runs the check for authenticated and unauthenticated requests alike, skipping it only where a valid share link has already bound the requested file to that link's page.	7.5	More Details

CVE-2026-81296	Unauthenticated Broken Access Control in Fluent Forms Pro Add On Pack <= 6.2.12 versions.	7.5	More Details
CVE-2026-81297	Subscriber Privilege Escalation in Fluent Forms Pro Add On Pack <= 6.2.12 versions.	7.5	More Details
CVE-2026-81767	Unauthenticated Broken Access Control in Simple Payment <= 2.5.2 versions.	7.5	More Details
CVE-2026-82638	jina-ai reader disables its private-address guard outside Google Cloud deployments, allowing unauthenticated attackers to perform server-side request forgery. Attackers can supply publicly resolvable hostnames mapping to private addresses to retrieve cloud metadata and internal service content.	7.5	More Details
CVE-2026-47851	Analyzing a PDF with a deeply nested or cyclic table of contents can cause a StackOverflowError in the ingestion thread. Spring AI 2.0.0 Spring AI 1.1.0 - 1.1.8 Spring AI 1.0.0 - 1.0.9	7.5	More Details
CVE-2026-71257	Apache Wicket enforces the upload limits configured on a form or upload field while parsing a multipart request with Apache Commons FileUpload. If the request body has already been consumed by another component, Commons FileUpload returns no items and Wicket falls back to reading the upload through HttpServletRequest#getParts(). The per-file size limit (for example Form#setFileMaxSize) and the file count limit (Form#setFileCountMax) are not applied to the parts obtained that way, and no exception is raised, so the upload is processed as though those limits had been satisfied. A remote uploader can therefore submit files that are larger, or more numerous, than the application permits, up to whatever the component that parsed the request allows. A part carrying no Content-Type header is additionally read into memory in full during parsing, so the size of that allocation is determined by the request and bounded only by those same external limits. The total upload size limit (Form#setMaxSize) is not affected. Commons FileUpload compares the declared Content-Length against it before reading the body, so a request declaring an oversized length is rejected before the fallback is reached. The fallback is reached in deployments where a servlet or filter has already parsed the request body — for example a servlet annotated with @MultipartConfig, Spring Boot's multipart resolver, or any filter that calls HttpServletRequest#getParameter() on a multipart request. It applies to the Wicket components that accept uploads on that path, including Form with FileUploadField, FileUploadToResourceField and AjaxFileDropBehavior. Applications that configure neither a per-file nor a file-count limit are not affected, as Wicket applies neither by default. This issue affects Apache Wicket: from 8.0.0 through 8.18.0, from 9.0.0 through 9.23.0, from 10.0.0 through 10.10.0. Users are recommended to upgrade to version 8.19.0, 9.24.0 or 10.11.0, which fix the issue. Users of Apache Wicket 7.x or older, which are no longer supported, should upgrade to a supported version. As a workaround, configure equivalent limits in the component that parses the request — for example spring.servlet.multipart.max-file-size and max-request-size, or maxFileSize and maxRequestSize in @MultipartConfig or in the web.xml <multipart-config> element.	7.5	More Details
CVE-2026-51627	Incorrect access control in the getIptvCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain IPTV and IGMP configuration information via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	7.5	More Details
CVE-2026-51673	Incorrect access control in the setNtpCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to alter time synchronization settings via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	7.5	More Details
CVE-2026-51671	Incorrect access control in the getCloudDownloadStatus function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain cloud firmware download state information via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	7.5	More Details
CVE-2026-75328	In DocSys-master V2.02.85, the downloadDocEx interface in src/com/DocSystem/controller/DocController.java has an arbitrary file read vulnerability:	7.5	More Details
CVE-2026-51668	Incorrect access control in the setLanguageCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to modify language configuration via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	7.5	More Details
CVE-2026-19616	Missing Authorization vulnerability in TBC Technology Inc. KitLogistic allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects KitLogistic: before v2.2.2.	7.5	More Details
CVE-2026-82880	YaCy Search Server through 1.941 contains an XML external entity injection vulnerability in SVG, FreeMind, and OpenSearch parsers that fail to disable external entity resolution. Attackers can publish malicious documents with DOCTYPE declarations containing SYSTEM entities pointing to local files, causing the crawler to exfiltrate file contents into the searchable index.	7.5	More Details
CVE-2026-51695	Incorrect access control in the setDdnsCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to alter dynamic DNS state via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	7.5	More Details
CVE-2026-51641	Incorrect access control in the getWiFiMeshConfig function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain mesh configuration and runtime state information via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	7.5	More Details

CVE-2026-18884	The WooCommerce Lottery plugin for WordPress is vulnerable to Time-Based SQL Injection via 'orderby' and 'order' GET Parameters in all versions up to, and including, 2.2.9 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details
CVE-2026-51642	Incorrect access control in the getMeshRoutingTable function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain mesh routing information via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	7.5	More Details
CVE-2026-51644	Incorrect access control in the getCrpcConfig function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain cloud remote-control status and URL information via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	7.5	More Details
CVE-2026-51647	Incorrect access control in the getCrpcCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain cloud remote-control status and URL information via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	7.5	More Details
CVE-2026-51648	Incorrect access control in the getWanInfo function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain WAN information returned by the endpoint via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	7.5	More Details
CVE-2026-75333	yx-image-recognition v1.0 is vulnerable to Path Traversal. Parameters such as dir, filePath are directly passed to new File() for file system operations without any path sanitization or whitelist validation.	7.5	More Details
CVE-2026-51625	Incorrect access control in the getWiFiEasyCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain sensitive information such as SSIDs and Wi-Fi keys, via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	7.5	More Details
CVE-2026-51624	Incorrect access control in the getStationMacByIp function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain a client MAC address via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	7.5	More Details
CVE-2026-51617	Incorrect access control in the getSysStatusCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain sensitive information such as operation mode, firmware version, serial number, WAN/LAN IP addresses, WiFi SSID, encryption keys, and connected client statistics via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	7.5	More Details
CVE-2026-51623	Incorrect access control in the getDdnsStatus function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain DDNS runtime status and public IP information via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	7.5	More Details
CVE-2026-51621	Incorrect access control in the getInitCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain sensitive device configuration information via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	7.5	More Details
CVE-2026-51620	Incorrect access control in the getNetInfoCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain network topology and interface configuration information via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	7.5	More Details
CVE-2026-51615	Incorrect access control in the getLanCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain LAN addressing and DHCP configuration information via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	7.5	More Details
CVE-2026-51619	Incorrect access control in the getOnlineClient function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain online client information via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	7.5	More Details
CVE-2026-51618	Incorrect access control in the getWizardCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain setup wizard and onboarding configuration information via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	7.5	More Details
CVE-2026-76763	A flaw was found in SmallRye GraphQL. The number scalar coercion for BigInteger does not properly validate the magnitude of float or string inputs. An unauthenticated remote attacker can exploit this by sending a GraphQL query containing a large exponent float literal. This can lead to the allocation of extremely large BigInteger objects, causing CPU exhaustion or an OutOfMemoryError, resulting in a denial of service.	7.5	More Details
CVE-2026-51694	Incorrect access control in the setStaticDhcpRules function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to add or change static DHCP rules via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	7.5	More Details
CVE-2026-51616	Incorrect access control in the getWanIeCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain LAN addressing and DHCP configuration information via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	7.5	More Details

CVE-2026-82595	A vulnerability was found in D-Link DIR-825M 1.1.8. Affected by this vulnerability is the function sub_456CF4 of the file /boafrm/formSysCmd of the component System Command Execution. Performing a manipulation of the argument sysCmd results in command injection. It is possible to initiate the attack remotely. The exploit has been made public and could be used.	7.4	More Details
CVE-2026-59288	The GraphiQL page bundled with Spring for GraphQL sends requests to the GraphQL endpoints of the application. An attacker can share a malicious URL so that the victim's browser might leak confidential information to the attacker's website. Spring for GraphQL 2.0.0 - 2.0.4 Spring for GraphQL 1.4.0 - 1.4.6 Spring for GraphQL 1.1.0 - 1.3.9 Spring for GraphQL 1.0.0 - 1.0.7	7.4	More Details
CVE-2026-18717	ASE2000 2.35 through 2.37 is vulnerable to an improper certificate validation vulnerability, which may allow an attacker to impersonate the trusted peer, complete the TLS handshake, and read or modify protected communications.	7.4	More Details
CVE-2026-82597	A vulnerability was identified in TOTOLINK NR1800X 9.1.0u.6681_B20230703. This affects the function setUssd of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument ussd leads to command injection. The attack can be initiated remotely. The exploit is publicly available and might be used.	7.4	More Details
CVE-2026-54550	IzPack is a widely used tool for packaging applications on the Java platform as cross-platform installers. In 5.2.6 and earlier, UnpackerBase.unpack() in izpack-installer/src/main/java/com/izforge/izpack/installer/unpacker/UnpackerBase.java obtains an attacker-controlled PackFile targetPath, passes it through IoHelper.translatePath(), which only converts separators, and constructs a File without normalizing parent-directory segments or enforcing destination containment. A malicious installer pack entry containing ../ sequences can therefore write outside the intended installation directory to startup folders, executable search paths, or other locations accessible with the victim's privileges when the victim runs the installer.	7.4	More Details
CVE-2026-82608	A vulnerability was determined in Kamailio up to 5.5.0/6.0.7. This affects the function get_4bytes of the file src/modules/ims_registrar_scscf/cxdx_avp.c of the component AVP Handler. Executing a manipulation can lead to out-of-bounds read. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized. This patch is called abb5d60af6eefbd367bf6588c5589566b090e272. It is advisable to implement a patch to correct this issue. The vendor points out, that "[v]ersion 5.5.0 is old and not maintained anymore."	7.4	More Details
CVE-2026-40018	None None None No publicly available exploits are known.	7.4	More Details
CVE-2026-82480	A security flaw has been discovered in NASA cFS up to 7.0.1. The affected element is the function CFE_SB_GetUserDataLength of the file src/cFS/cfe/modules/sb/fsw/src/cfe_sb_util.c of the component cFE Software Bus. Performing a manipulation of the argument TotalMsgSize/HdrSize results in integer underflow. It is possible to initiate the attack remotely. The vendor was contacted early about this disclosure but did not respond in any way.	7.4	More Details
CVE-2026-82281	Kotaemon through 0.12.0 fails to properly validate conversation ownership in select_conv, delete_conv, rename_conv, and on_set_public_conversation functions in control.py. Attackers can read other users' chat histories, delete conversations, or rename conversations by supplying arbitrary conversation identifiers without proper authorization checks.	7.4	More Details
CVE-2026-73208	An attacker that holds a token intended for a different purpose can authenticate, because when an OAuth2 token response does not contain a scope claim, the audience claim is used in its place and checked against the configured required scopes. These are different concepts, and the audience claim does not describe what a token is allowed to do. A token that grants no relevant permissions can be accepted because its intended recipient value happens to match a configured scope name, granting access that should have been denied. It also hides an identity provider misconfiguration where scopes are not being issued at all. Ensure the identity provider issues a scope claim for all tokens used with Dovecot, and that configured scope names do not match audience values. Update to non-vulnerable version. No publicly available exploits are known.	7.4	More Details
CVE-2026-47841	An application using Spring Security's WebAuthn support may be vulnerable to user verification bypass when using a distributed HTTP session store. Spring Security 7.1.0 Spring Security 7.0.0 - 7.0.6 Spring Security 6.5.0 - 6.5.11 Spring Security 6.4.0 - 6.4.18	7.4	More Details
CVE-2026-82289	Gitingest through 0.3.1 fails to properly validate hostnames in _validate_host, accepting any host with a git., gitlab., or github. prefix regardless of known-hosts list membership. Attackers can submit URLs with attacker-controlled hostnames to trigger outbound connections to arbitrary hosts and disclose GitHub personal access tokens via HTTP basic credentials.	7.4	More Details
CVE-2026-81020	wolfEngine before 1.4.1 generates the 8-byte explicit AES-GCM nonce once when the TLS write key is set and never increments it per record. As a result every TLS 1.2 and DTLS 1.2 AES-GCM record within a connection is encrypted under an identical key and nonce pair. Reusing a GCM key and nonce discloses the keystream (the XOR of two ciphertexts equals the XOR of their plaintexts, so one known record recovers the others) and leaks the GHASH authentication key, enabling authentication tag forgery. AES-CCM, TLS 1.3, and non-TLS use of the cipher are not affected.	7.4	More Details
	wolfProvider before 1.2.2 generates the 8-byte explicit AES-GCM nonce once when the TLS write key is set		

CVE-2026-81019	and never increments it per record. As a result every TLS 1.2 and DTLS 1.2 AES-GCM record within a connection is encrypted under an identical key and nonce pair. Reusing a GCM key and nonce discloses the keystream (the XOR of two ciphertexts equals the XOR of their plaintexts, so one known record recovers the others) and leaks the GHASH authentication key, enabling authentication tag forgery. AES-CCM, TLS 1.3, and non-TLS use of the cipher are not affected.	7.4	More Details
CVE-2026-82543	A vulnerability was detected in vastsa FileCodeBox up to 2.3. This vulnerability affects the function update_file_usage of the file apps/base/views.py of the component Pickup Limit Handler. Performing a manipulation results in race condition. It is possible to initiate the attack remotely. The exploit is now public and may be used. Upgrading to version 2.5.0 is able to resolve this issue. The patch is named 8d7d856c62d73badd0797eb4daec8d2ff10a403a. Upgrading the affected component is recommended.	7.3	More Details
CVE-2026-82610	A security flaw has been discovered in itsourcecode Online Medicine Delivery System 1.0. Affected is the function Employee::employeeAuthentication of the file /rider/login.php of the component Login Interface. The manipulation of the argument emp_email results in sql injection. It is possible to launch the attack remotely. The exploit has been released to the public and may be used for attacks.	7.3	More Details
CVE-2026-81203	A vulnerability has been found in SourceCodester Simple Online Food Ordering System 1.0. This affects an unknown function of the file /admin/ajax.php?action=login2. The manipulation of the argument email leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2026-81202	A flaw has been found in itsourcecode Payroll System 1.0. The impacted element is the function create/read/update/delete of the file ajax.php of the component CRUD Operation Handler. Executing a manipulation of the argument action can lead to missing authentication. The attack may be performed from remote. The exploit has been published and may be used.	7.3	More Details
CVE-2026-18252	GitLab has remediated an issue in GitLab EE affecting all versions from 18.9 before 19.1.7, 19.2 before 19.2.5, and 19.3 before 19.3.1 that, under certain conditions, an authenticated user with developer-role permissions could have executed arbitrary commands in a CI context, due to the Claude agent processing configuration from a user-controlled source.	7.3	More Details
CVE-2026-82612	A security vulnerability has been detected in itsourcecode Online Medicine Delivery System 1.0. Affected by this issue is the function loadResultList of the file /index.php?q=single-item of the component Product Detail Page. Such manipulation of the argument ID leads to sql injection. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2026-82611	A weakness has been identified in itsourcecode Online Medicine Delivery System 1.0. Affected by this vulnerability is the function Customer::cusAuthentication of the file /login.php of the component Customer Login Interface. This manipulation of the argument U_USERNAME causes sql injection. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks.	7.3	More Details
CVE-2026-82701	A vulnerability was determined in code-projects Online Shopping System 1.0. Affected by this issue is some unknown functionality of the file /action.php of the component Search Functionality. This manipulation of the argument keyword causes sql injection. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2026-82613	A vulnerability was detected in itsourcecode Online Medicine Delivery System 1.0. This affects the function loadResultList of the file /index.php?q=product of the component Product Search Interface. Performing a manipulation of the argument Search results in sql injection. The attack may be initiated remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2026-82614	A flaw has been found in itsourcecode Online Medicine Delivery System 1.0. This vulnerability affects the function loadResultList of the file /index.php?q=product of the component Product Category Filter Interface. Executing a manipulation of the argument Category can lead to sql injection. The attack may be launched remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2026-82615	A vulnerability has been found in itsourcecode Online Medicine Delivery System 1.0. This issue affects the function Customer::find_phone of the file /passwordrecover.php of the component Password Recovery Interface. The manipulation of the argument phonenumber leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2026-82621	A weakness has been identified in Soarkey StudentManagement and 学生信息管理系统 up to e08f7f1d5015af407aa4cca0ada3dea189b4937e. This impacts the function AdminDao.doGet of the file code/src/service/AdminDao.java of the component Administrative Servlet. Executing a manipulation of the argument action can lead to authorization bypass. It is possible to launch the attack remotely. The exploit has been made available to the public and could be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-82630	A vulnerability was identified in PowerJob up to 5.1.2. Impacted is the function MuConnectionManager.getOrCreateConnection of the file powerjob-server/powerjob-server-starter/src/main/java/tech/powerjob/server/web/controller/TestController.java of the component Transport Endpoint. The manipulation leads to server-side request forgery. The attack is possible to be carried out remotely. The exploit is publicly available and might be used. The project was informed of the problem early	7.3	More Details

	through an issue report but has not responded yet.		
CVE-2026-80664	In the Linux kernel, the following vulnerability has been resolved: netfilter: xt_nat: reject unsupported target families xt_nat SNAT and DNAT target handlers assume IP-family conntrack state is present and can dereference a NULL pointer when instantiated from an unsupported family through nft_compat. A bridge-family compat rule can therefore trigger a NULL-dereference in nf_nat_setup_info(). Reject non-IP families in xt_nat_checkentry() so unsupported targets cannot be installed. Keep NFPROTO_INET allowed for valid inet NAT compat users and leave the runtime fast path unchanged. [The crash was fixed via 9dbba7e694ec ("netfilter: nft_compat: ebtables emulation must reject non-bridge targets"), so this patch is no longer critical. Nevertheless, NAT is only relevant for ipv4/ipv6, so this extra family check is a good idea in any case.]	7.3	More Details
CVE-2026-82607	A vulnerability was found in Cozmoslabs Profile Builder Plugin up to 3.16.1 on WordPress. The impacted element is the function wppb_ajax_simple_avatar of the file /wp-admin/admin-ajax.php of the component Avatar Simple Upload AJAX Handler. Performing a manipulation results in unrestricted upload. The attack is possible to be carried out remotely. The exploit has been made public and could be used. Upgrading to version 3.16.2 is sufficient to resolve this issue. It is suggested to upgrade the affected component.	7.3	More Details
CVE-2026-82801	A vulnerability was detected in NASA earthdata-search 1.0.0. Affected by this vulnerability is the function scaleImage of the file serverless/src/scaleImage/handler.js of the component scale Endpoint. Performing a manipulation results in server-side request forgery. The attack can be initiated remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-82668	A security vulnerability has been detected in klaussilveira GitList 2.0.0. Affected by this vulnerability is the function getDefaultBranch of the file src/SCM/System/Git/CommandLine.php of the component Git Command Line. Such manipulation leads to os command injection. The attack can be executed remotely. The exploit has been disclosed publicly and may be used. Upgrading to version 3.0.0-beta addresses this issue. The name of the patch is 88cf2866083d5f7c20d9d565c45f828a7ad1516b. Upgrading the affected component is advised.	7.3	More Details
CVE-2026-82808	A vulnerability was identified in Inbox Foundry ActiveInbox Extension up to 7.10.24 on Chrome. Impacted is an unknown function of the file dist/service-worker.production-esm.js of the component Google OAuth Client Secret. Such manipulation leads to hard-coded credentials. The attack can be executed remotely. The exploit is publicly available and might be used. The vendor was informed beforehand about the issue. The support explains, that "[a]t the moment, the [bug bounty] programme is on hold while we work through a large number of existing reports."	7.3	More Details
CVE-2026-82478	A vulnerability was determined in NASA Trick 19.6.0. This issue affects the function JSONVariableServerThread::parse_request of the file trick_source/sim_services/JSONVariableServer/JSONVariableServerThread.cpp of the component TCP Socket Handler. This manipulation causes stack-based buffer overflow. The attack is possible to be carried out remotely. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-80578	In the Linux kernel, the following vulnerability has been resolved: fbdev: core: Fix pointer desynchronization in fb_io_read() In fb_io_read(), if copy_to_user() performs a partial copy (e.g., due to a faulty user buffer), the loop adjusts the chunk size 'c' and updates the remaining 'count'. However, the hardware 'src' pointer has already been eagerly advanced by the original chunk size. If the loop is allowed to continue, the read will resume from an incorrect, over-advanced offset. Since the remaining 'count' was only decremented by the successful bytes, this desynchronization causes the next iterations to execute more hardware reads than originally bounded, eventually leading to out-of-bounds I/O reads. Fix this by breaking out of the loop immediately upon a partial copy_to_user(). A partial copy indicates a faulty user buffer, making subsequent read attempts futile. Breaking out ensures we return the number of successfully read bytes without risking out-of-bounds hardware accesses in subsequent mismatched iterations.	7.3	More Details
CVE-2026-81491	A flaw has been found in boxpositron with-context-mcp up to 3.0.7. This affects the function ingest_notes/teleport_notes/sync_notes/project_folder of the file src/index.ts. Executing a manipulation can lead to path traversal. It is possible to launch the attack remotely. The exploit has been published and may be used. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-81421	A security flaw has been discovered in ddfourtwo sentry-selfhosted-mcp 0.4.0. The affected element is an unknown function of the component raw_sentry_api. The manipulation of the argument endpoint results in server-side request forgery. It is possible to launch the attack remotely. The exploit has been released to the public and may be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	7.3	More Details
CVE-2026-82600	A security flaw has been discovered in SeaCMS up to 13.6. Affected by this issue is some unknown functionality of the file /zyapi.php?ac=videolist. Performing a manipulation of the argument ids results in sql injection. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks.	7.3	More Details
CVE-2026-	A flaw has been found in MegaEase EaseProbe up to 2.3.0. Affected is the function realIP of the file web/server.go of the component Middleware. This manipulation of the argument X-Forwarded-For/X-Real-IP/True-Client-IP causes improper access controls. The attack can be initiated remotely. The exploit has been	7.3	More

82815	published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.		Details
CVE-2026-81690	openssl-encrypt (pip package) before 1.4.9 contains a symlink-following flaw in its verify-usb v2 added-file allowlist scan. The scan enumerated the drive with rglob(), which in CPython does not descend into symlinked directories and treats the symlink as an ordinary directory, while O_NOFOLLOW on the hash side binds only the final path component. An evil-maid attacker with physical access to the removable drive could replace a tool-tree directory with a symlink to a copy containing byte-identical files plus a planted __pycache__/*.pyc file (which CPython loads in preference to recompiling the clean .py). The planted file is never enumerated, added_files stays 0, and verify-usb reports PASSED, resulting in code execution when the victim runs the portable install. Fixed in 1.4.9 (affects both 1.4.x and 1.5.x lines).	7.3	More Details
CVE-2026-82598	A vulnerability was determined in SeaCMS up to 13.6. Affected is the function parseIf of the file search.php of the component Template Engine. This manipulation of the argument searchtype causes code injection. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2026-78276	Editor PHP Object Injection in Fluent Boards Pro <= 2.0.11 versions.	7.2	More Details
CVE-2026-6176	The Customer Reviews for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the aggregated review form submission in versions up to and including 5.106.0. This is due to insufficient input sanitization and output escaping on user-supplied review comment text. The plugin accepts review submissions from unauthenticated users through the 'cr_local_forms_submit' AJAX action without sanitizing HTML content before storing it via wp_insert_comment(), and later renders this stored content on product pages through comment_text() without proper escaping. This makes it possible for unauthenticated attackers with a valid review form URL (obtainable through review reminder emails sent to customers who placed orders) to inject arbitrary web scripts in pages that will execute whenever a user accesses the affected product page.	7.2	More Details
CVE-2026-19760	The WP Fastest Cache – WordPress Cache Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via HTTP Host Header in all versions up to, and including, 1.5.0 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 requires the Polylang or Polylang Pro plugin to be active and the Combine JS option to be enabled, as these conditions trigger the vulnerable Host-header-to-URL code path that writes attacker-controlled script src values into the shared page-cache file served to all subsequent visitors.	7.2	More Details
CVE-2026-5934	The WP Rocket plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to, and including, 3.21.0.1. This is due to insufficient input sanitization and output escaping of user-supplied data via the rocket_beacon AJAX endpoint. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2026-78271	Editor Privilege Escalation in FluentCRM Pro <= 3.1.12 versions.	7.2	More Details
CVE-2026-81757	Author Remote Code Execution (RCE) in Rank Math SEO <= 1.0.276 versions.	7.2	More Details
CVE-2026-74851	The Pods WordPress plugin before 3.3.9.1 does not correctly compare a display callback against its list of blocked functions, allowing users with the author role and above to execute arbitrary code on the server. Only sites using the restricted display-callback mode are affected, which is the automatic default on installations whose first Pods version predates 3.1.	7.2	More Details
CVE-2026-13415	The CMP WordPress plugin before 4.1.18 does not enforce an option-name allow-list when importing settings via one of its AJAX actions, allowing users with the Editor role (when the administrator has granted the Editor role access to the CMP WordPress plugin before 4.1.18's admin-bar controls) to update arbitrary WordPress options, including options that lead to privilege escalation to Administrator.	7.2	More Details
CVE-2026-19223	The Smush WordPress plugin before 4.3.2 does not restrict a network-wide setting to network administrators, allowing an administrator of any single site on a multisite network to execute arbitrary code across the entire network.	7.2	More Details
CVE-2026-75121	PLANET GS-4210-16P2S V3 firmware before 3.441b260626 contains an authenticated OS command injection vulnerability in /cgi-bin/dispatcher.cgi. The web_vlan_membership_edit_dialog_post handler incorporates the memberTags POST parameter into a shell command without sanitization. A remote authenticated attacker can send a crafted memberTags value to execute arbitrary operating-system commands on the device.	7.2	More Details
CVE-2026-80233	CAYIN CMS-WS, CMS-SE, and SMP series products developed by CAYIN Technology have an Arbitrary File Upload vulnerability. Privileged remote attackers can upload and execute web shells backdoors, thereby enabling arbitrary code execution on the server.	7.2	More Details
CVE-2026-	The Formidable Forms – WordPress Form Builder for Contact Forms, Calculators, Quizzes & More plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'frm_user_id' parameter in all versions up to, and including, 6.33.1 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		More

18331	accesses an injected page. By forging frm_user_id to match an administrator's user ID — discoverable via the public WordPress REST API — an unauthenticated attacker causes wp_kses_post() to serve as the only output filter, which preserves the injected payload structurally intact; the plugin's admin JavaScript then decodes and executes it automatically on page load.	7.2	Details
CVE-2026-75122	PLANET GS-4210-16P2S V3 firmware before 3.441b260626 contains an authenticated OS command injection vulnerability in /cgi-bin/httpuploadcert.cgi. The certificate password field in a certificate upload request is incorporated into a shell command without sanitization of shell metacharacters. A remote attacker with administrator web credentials can submit a crafted certificate upload request to execute arbitrary operating-system commands on the device.	7.2	More Details
CVE-2026-18324	The Forminator Forms – Contact Form, Payment Form & Custom Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Rich-Text Textarea Field in all versions up to, and including, 1.57.0.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Exploitation requires that the targeted Textarea field has the Rich-Text editor option enabled.	7.2	More Details
CVE-2026-71171	Dell Cloud Disaster Recovery, versions 20.2 and prior, contain an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in the REST API. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Remote execution.	7.2	More Details
CVE-2026-75417	A SQL injection vulnerability was found in YzmCMS 7.5. The issue occurs in the get_arrchildid() function within application/admin/controller/category.class.php, where the user-controlled parentid parameter is concatenated directly into a FIND_IN_SET() SQL clause without proper sanitization. This allows an authenticated administrator to execute arbitrary SQL queries via boolean-based blind injection, potentially leading to full database compromise.	7.2	More Details
CVE-2026-81031	IDURAR ERP CRM changes the password of whichever account a request names rather than the account making the request. The update handler in backend/src/controllers/middlewaresControllers/createUserController/updatePassword.js resolves the authenticated user from the request that the token middleware populated, then issues its update against a filter built from the identifier in the URL path, and never compares the two. The route is mounted behind the administrator token check only, so any valid administrator session is sufficient, and the sole ownership-like guard in the handler rejects a single hardcoded demo address. A caller can therefore set an arbitrary password on any other administrator account and sign in as it. The read handler in the same controller directory accepts an identifier the same way, which supplies the identifiers needed to pick a target.	7.2	More Details
CVE-2026-18978	The LiteSpeed Cache plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Comment Content in all versions up to, and including, 7.8.1 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. A comment payload crafted exclusively from decimal numeric character references (e.g. ", <, >) placed inside an allowed element such as <code> bypasses WordPress's wp_kses sanitization, as kses does not treat a data-settings="..." substring within text content as an HTML attribute, allowing the malicious payload to reach the vulnerable function. For this to be exploitable, the site must allow users with previously approved comments to write new comments, and the require_name_email setting must be disabled.	7.2	More Details
CVE-2026-76053	The TranslatePress – Translate Multilingual sites with AI Translation plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Comment Noise-Key Injection into HTML Parser in all versions up to, and including, 3.3.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Exploitation is possible because WordPress's comment KSES allowlist permits the payload structure — an anchor tag with href and title attributes alongside a code tag — causing the malicious comment to be stored verbatim in the database, where it is later processed by the vulnerable parser during page translation.	7.2	More Details
CVE-2026-77365	The Optimole – Optimize Images | Convert WebP & AVIF | CDN & Lazy Load | Image Optimization plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'a' (above_fold_images) parameter in all versions up to, and including, 4.2.10 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2026-14558	The User Frontend WordPress plugin before 4.3.10 does not properly validate field type definitions and deserialises user-controlled post metadata when rendering submitted posts, allowing users with Editor-level access and above to inject arbitrary PHP objects, which can lead to remote code execution when a suitable POP chain is present on the site.	7.2	More Details
	The Booking for Appointments and Events Calendar – Amelia plugin for WordPress is vulnerable to Stored Cross-Site Scripting via customer name fields in versions up to and including 2.2. This is due to an authentication bypass where the AddBookingCommand explicitly skips nonce verification (Command.php line 186), allowing unauthenticated users to submit booking data. While the plugin applies sanitize_text_field() to customer firstName and lastName fields (BookingApplicationService.php lines 302-		

CVE-2026-6286	308), this function only removes HTML tags and preserves special characters including double quotes. The vulnerability manifests in the administrative Calendar view where a FullCalendar eventContent callback interpolates customer names directly into JavaScript template literals (redesign/dist/index.js line 199) and renders them via innerHTML without proper HTML entity encoding. Because double quotes are preserved, an attacker can inject payloads like '" onmouseover="alert(document.cookie)"' to break out of the title attribute and inject malicious event handlers. This makes it possible for unauthenticated attackers to inject arbitrary web scripts that will execute when an administrator accesses the Calendar page and hovers over the malicious appointment.	7.2	More Details
CVE-2026-79996	The User Registration & Membership WordPress plugin before 5.2.6 does not perform a capability check when saving its login settings, allowing authenticated users who have been granted a User Registration & Membership WordPress plugin before 5.2.6 management capability but not full administrator access to change arbitrary site options and escalate their privileges to administrator.	7.2	More Details
CVE-2026-47836	The base directory (spring.cloud.config.server.svn.basedir) used by the Spring Cloud Config Server to clone SVN repositories to is susceptible to time-of-check-time-of-use (TOCTOU) attacks. Spring Cloud Config 5.0.0 - 5.0.4 Spring Cloud Config 4.3.0 - 4.3.4 Spring Cloud Config 4.0.0 - 4.2.8 Spring Cloud Config 3.1.14 and earlier	7.2	More Details
CVE-2026-36102	An issue in the inviteController.js component in Bluewave Labs Checkmate <=3.3.0 allows remote authenticated administrators to escalate privileges to superadmin via the role parameter to the /api/v1/invite endpoint.	7.2	More Details
CVE-2026-75123	PLANET GS-4210-16P2S V3 firmware before 3.441b260626 contains an authenticated OS command injection vulnerability in /cgi-bin/dispatcher.cgi. The web_smtp_test_post handler incorporates a caller-supplied SMTP server value directly into a shell command without sanitization. A remote attacker with administrator web credentials can send a crafted SMTP server value to execute arbitrary operating-system commands on the device.	7.2	More Details
CVE-2026-54718	Silverstripe Advanced Workflow is a highly configurable step-based workflow module. Prior to 6.4.5, 7.1.3, and 7.2.1, an attacker with permission to author the advanced workflow email template can place a specially crafted server-side template payload in NotifyUsersWorkflowAction.EmailTemplate. When NotifyUsersWorkflowAction renders the field through the Silverstripe template engine SSTemplateParser, the payload can cause PHP evaluation and arbitrary code execution on the server; the regression coverage is in tests/php/WorkflowEngineTest.php. This issue is fixed in versions 6.4.5, 7.1.3, and 7.2.1.	7.2	More Details
CVE-2026-80675	In the Linux kernel, the following vulnerability has been resolved: libbpf: Reject non-exclusive metadata maps in the signed loader The loader verifies map->sha against the metadata hash in its instructions. map->sha is calculated when BPF_OBJ_GET_INFO_BY_FD is called on the frozen map. While the map is frozen, the /signed loader/ must also ensure the map is exclusive, as, without exclusivity (which a hostile host could just omit when loading the loader), another BPF program with map access can mutate the contents afterwards, so the check passes on stale data. With the extra check as part of the signed loader, it now refuses to move on with map->sha validation if the host set it up wrongly.	7.1	More Details
CVE-2026-55066	Vikunja is an open-source self-hosted task management platform. Prior to 2.4.0, POST /api/v1/projects/{project}/views/{view}/buckets/{bucket}/tasks accepts a body supplied task_id but TaskBucket.CanUpdate in pkg/models/kanban_task_bucket.go authorizes only the project, view, and bucket from the URL. updateTaskBucket then calls Task.ReadOne without a separate task permission check, returns the victim task contents, and can update the task done state when the attacker chooses a done bucket. Because task identifiers are global sequential values, an authenticated user can enumerate cross-tenant tasks and modify their completion metadata through both the v1 and v2 routes that share this model. This issue is fixed in version 2.4.0.	7.1	More Details
CVE-2026-81765	Unauthenticated Cross Site Scripting (XSS) in Tailored Tools <= 3.0.2 versions.	7.1	More Details
CVE-2026-81764	Unauthenticated Cross Site Scripting (XSS) in Email Essentials <= 6.0.6 versions.	7.1	More Details
CVE-2026-81298	Unauthenticated Cross Site Scripting (XSS) in LeadConnector <= 4.0.5 versions.	7.1	More Details
CVE-2026-54085	Wazuh is an open-source security platform providing unified XDR and SIEM protection for endpoints and cloud workloads. In versions 4.2.0 through 4.14.6, multiple active response scripts pass attacker-influenced alert fields to privileged system commands without validating their format, allowing argument injection into tools that run as root. Five of the eight scripts that handle the srcip field, route-null.c, netsh.c, pf.c, npf.c, and ipfw.c, omit the get_ip_version() check that rejects non-IP input, and disable-account.c passes the dstuser field to passwd/chuser with only a comparison against "root". An attacker who can inject crafted log events, for example via syslog, can supply srcip or dstuser values that, when an active response rule triggers, are passed unvalidated to firewall and account-management commands such as pfctl, npfctl, ipfw, route, netsh, and passwd. This enables injecting additional command arguments, and on Windows the unquoted CreateProcess command-line concatenation in wpopenv() lets a srcip containing spaces add further arguments, while disable-account.c can be abused to lock arbitrary system accounts. This issue is	7.1	More Details

	fixed in version 4.14.7.		
CVE-2026-82455	RubyGems fails to re-validate path containment after filesystem symlink resolution during gem extraction. When a pre-existing symlink inside the destination directory points outside the extraction root, extracted files that appear to be written under the destination directory can instead be written outside of it, breaking the extraction safety boundary. The fix resolves the real path of the parent directory before writing and raises Gem::Package::PathError if it escapes the destination directory.	7.1	More Details
CVE-2026-81934	Redis contains a use-after-free vulnerability in the 'tlsProcessPendingData()' function, which handles the TLS pending-data list if Redis is configured with TLS support. A remote, unauthenticated attacker may be able to execute arbitrary commands with the privileges of the Redis server.	7.1	More Details
CVE-2026-81291	Unauthenticated Cross Site Scripting (XSS) in Uncode <= 2.12.7 versions.	7.1	More Details
CVE-2026-81290	Unauthenticated Cross Site Scripting (XSS) in Email Subscribers & Newsletters <= 5.9.33 versions.	7.1	More Details
CVE-2026-82241	Budibase backend-core (@budibase/backend-core, as used by @budibase/server) omits the shared address space range 100.64.0.0/10 from its default SSRF blacklist (DEFAULT_BLACKLIST) used by REST datasource query previews. When the default blacklist is active (i.e., a self-hosted deployment has not defined BLACKLIST_IPS), an authenticated user with the Builder permission can submit a REST datasource query preview request to POST /api/queries/preview targeting a reachable HTTP(S) service in the 100.64.0.0/10 range, causing the server to send a request to that target and return its response through the preview flow. Per the advisory, no released fix was identified at the time of publication; remediation is to add 100.64.0.0/10 to DEFAULT_BLACKLIST.	7.1	More Details
CVE-2026-82246	Budibase Server before 3.41.3 contains a server-side request forgery vulnerability in the query import endpoint that fails to validate user-supplied URLs before fetching content. Attackers can submit arbitrary URLs to retrieve responses from internal services including cloud metadata endpoints and other restricted network resources.	7.1	More Details
CVE-2026-81838	A relative path traversal issue in the zip extraction functionality in AWS diagram-as-code (awsdac) in versions 0.10 through 0.23 can allow a third party to write arbitrary files to the local filesystem via crafted zip entry names containing path traversal sequences. This could allow the third party to perform inappropriate actions in the diagram bundle. To remediate this issue, users should upgrade to the version 0.24 or later.	7.1	More Details
CVE-2026-79747	MCPHub is a unified hub for centrally managing and dynamically orchestrating multiple MCP servers/APIs into separate endpoints with flexible routing strategies. Prior to version 1.0.32, an authenticated non-admin user can register a server pointing at an arbitrary URL and make the hub issue server-side requests to it, with no egress filtering (no block of loopback / RFC1918 / link-local 169.254.0.0/16). Via the OpenAPI proxy path the response body is returned to the caller (full, reflected SSRF); via the SSE/streamable-http transport the request is sent blind. This issue has been patched in version 1.0.32.	7.1	More Details
CVE-2026-81529	Improper neutralization of delimiters in connection-URL construction allows connection-option injection in the MongoDB C# Driver. When an application passes untrusted text into the driver's connection-URL builder and round-trips the builder back into a client configuration, the untrusted text is serialized without neutralizing the URL/option delimiters and is then re-parsed as authoritative connection options. A low-privileged user of such an application can thereby introduce or suppress security-relevant connection settings.	7.1	More Details
CVE-2026-79745	MCPHub is a unified hub for centrally managing and dynamically orchestrating multiple MCP servers/APIs into separate endpoints with flexible routing strategies. Prior to version 1.0.32, the built-in prompt and resource controllers perform no role checking. The mutating POST/PUT /api/prompts* and POST/PUT /api/resources* routes are attached to the authenticated router with no admin gate, and the handlers never read req.user. The DAO singletons they write are consulted first — ahead of any connected MCP server — for every session in handleGetPromptRequest / handleReadResourceRequest. A non-admin can therefore create, overwrite, and shadow global prompt templates and resources that all other users are served. The scored impact is the unauthorized integrity violation (creation/tampering/shadowing of globally-served records); stored prompt injection into other users' LLM sessions is a downstream consequence of that tampering. This issue has been patched in version 1.0.32.	7.1	More Details
CVE-2026-81533	An application using the MongoDB BI Connector ODBC Driver may encounter a memory-safety issue when a submitted SQL statement contains an unusually long run of digits following a LIMIT clause. The issue occurs only on connections where the driver's optional prefetch setting is enabled, and stems from the driver copying the digit sequence into a fixed-size internal buffer without checking its length. A user able to influence the numeric portion of a LIMIT clause could cause the hosting application process to terminate unexpectedly or corrupt adjacent memory in that process.	7.1	More Details
CVE-2026-82648	WWBN AVideo contains a server-side request forgery filter bypass vulnerability in the isSSRFSafeURL function that fails to normalize NAT64 addresses written in hexadecimal form. Attackers can bypass SSRF protections by supplying hex-encoded NAT64 addresses like 64:ff9b::a9fe:a9fe to reach cloud metadata services and loopback interfaces.	7.1	More Details

CVE-2026-38821	A heap-based buffer overflow vulnerability exists in openNDS before 11.0.0 that allows an unauthenticated attacker on the captive portal network to crash the openNDS daemon (denial of service) and potentially achieve remote code execution. This is in http_microhttpd.c.	7.1	More Details
CVE-2026-82659	nodemailer before 9.0.1 fails to apply disableFileAccess and disableUrlAccess flags to message-level raw option, allowing authenticated attackers to read arbitrary files or perform server-side request forgery by supplying path or href properties. Attackers can exploit this by crafting raw messages with file paths or URLs that bypass the intended sandbox, with fetched content delivered in the outgoing message to attacker-controlled recipients.	7.1	More Details
CVE-2026-80662	In the Linux kernel, the following vulnerability has been resolved: cxl: Fix CXL_HEADERLOG_SIZE to match RAS Capability size The CXL r4.0 8.2.4.17.7 RAS Capability Structure has total length 0x58 bytes (CXL_RAS_CAPABILITY_LENGTH); the Header Log occupies the trailing 64 bytes at offset 0x18. CXL_HEADERLOG_SIZE was defined as SZ_512, eight times the actual on-device size. header_log_copy() reads CXL_HEADERLOG_SIZE_U32 (128) dwords from the RAS capability iomap, overrunning the 88-byte mapping by 448 bytes. The cxl_aer_uncorrectable_error trace event memcpy()s CXL_HEADERLOG_SIZE (512) bytes from its source. For the CPER caller the source is struct cxl_ras_capability_regs::header_log[16] (64 bytes) embedded in a stack-local cxl_cper_prot_err_work_data, so the memcpy reads 448 bytes of kernel stack into the trace event ring buffer where userspace can read it via tracefs. Set CXL_HEADERLOG_SIZE to 64 and derive CXL_HEADERLOG_SIZE_U32 from it, bringing all iomap readers into agreement on 16 dwords. Userspace tools such as rasdaemon have grown a dependency on the buggy 512-byte (128 u32) header_log layout in the cxl_aer_uncorrectable_error trace event. Add CXL_HEADERLOG_TRACE_SIZE_U32 = 128 and use it for the trace event __array and its memcpy to preserve that ABI. Both callers now pass a zero-filled u32[CXL_HEADERLOG_TRACE_SIZE_U32] staging buffer with only the first CXL_HEADERLOG_SIZE_U32 (16) entries populated from hardware; the remaining 112 u32s are zero-padded, keeping the 512-byte trace ring buffer layout intact. [dj: Replaced 64 with SZ_64 per RichardC]	7.1	More Details
CVE-2026-80663	In the Linux kernel, the following vulnerability has been resolved: tools/power/x86/intel-speed-select: Harden daemon pidfile open Avoid symlink-based pidfile clobbering by opening the pidfile with O_NOFOLLOW and validating it with fstat() before locking/writing. The daemon currently uses a fixed pidfile path under /tmp. A local unprivileged user can pre-create a symlink at that path and cause a root-run daemon instance to write into an attacker-chosen file.	7.1	More Details
CVE-2026-82280	Quivr through 0.0.322 fails to validate ownership in prompt endpoints, allowing authenticated users to modify any prompt by identifier. Attackers with read-only access to shared brains can read exposed prompt identifiers and overwrite system prompts affecting all brain users.	7.1	More Details
CVE-2026-81760	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Crocoblock JetEngine allows Reflected XSS. This issue affects JetEngine: from n/a through 3.8.14.2.	7.1	More Details
CVE-2026-81727	NLTK versions before 3.10.3 contain a filesystem containment bypass vulnerability in the Downloader.download and Downloader.incr_download methods that allows attackers to overwrite files outside the install root through pre-existing hardlinks. Attackers with write access to a shared downloader directory can create hardlinks pointing to outside-root files that are then overwritten during normal package extraction, mutating files outside the intended install tree.	7.1	More Details
CVE-2026-80685	In the Linux kernel, the following vulnerability has been resolved: mm/util: don't read __page_2 for order-1 folios in snapshot_page() snapshot_page() currently reads __page_2 after checking nr_pages > 1, but it should only do so when nr_pages > 2. If an order-1 folio is allocated at the end of a vmemmap section, __page_2 will not exist and reading it will cause a fault. During DLPAR memory remove on a 22 TB ppc64le LPAR, snapshot_page() oopsed on the page isolation path while reading an order-1 folio's __page_2 from an adjacent absent section (unmapped vmemmap). Fix this to avoid reading memmap that doesn't exist (e.g., a vmemmap hole).	7.1	More Details
CVE-2026-80665	In the Linux kernel, the following vulnerability has been resolved: KVM: arm64: nv: Inject SEA if kvm_translate_vncr() can't resolve PFN kvm_handle_vncr_abort() assumes that s1_walk_result conveys an abort when kvm_translate_vncr() returns -EFAULT. This is not always the case as it's possible to encounter 'late' failures on the output of S1 translation, e.g. a GFN outside of the memslots. Fix it by preparing an external abort before returning from kvm_translate_vncr(). Get rid of the BUG_ON() in the fault injection path while at it.	7.1	More Details
CVE-2026-14307	The geotargetingwp WordPress plugin before 3.5.6.2 does not sanitise or escape several parameters before reflecting them back in AJAX responses that are served with an HTML content type, allowing unauthenticated attackers to inject arbitrary web scripts that execute when a victim is tricked into submitting a crafted request.	7.1	More Details
CVE-2026-81768	Unauthenticated Cross Site Scripting (XSS) in Super Store Finder <= 7.10 versions.	7.1	More Details
CVE-2026-78261	Unauthenticated Cross Site Scripting (XSS) in Realtyna Organic IDX plugin <= 5.4.1 versions.	7.1	More Details
CVE-2026-	In the Linux kernel, the following vulnerability has been resolved: xfs: propagate errors from xfs_rtginode_load xfs_rtginode_ensure() treats every xfs_rtginode_load() error other than -ENOENT as success. This can leave the realtime group inode unset after an I/O, allocation, or corruption error. Growfs	7.1	More

80538	then continues as though the inode had been loaded. Only -ENOENT means that the inode needs to be created. Return all other errors to the growfs caller.		Details
CVE-2026-80523	In the Linux kernel, the following vulnerability has been resolved: clk: spacemit: k3: set hdma clock as critical HDMA clock is responsible for the internal TCM access path of X100 RISC-V core, so set the clock flag as critical to prevent it from being shut off, otherwise the Linux system will hang, for example in the case of a vector instruction access generates a page fault.	7.1	More Details
CVE-2026-80426	FiftyOne renders a dataset field's description as markup. The sidebar field-information component at app/packages/core/src/components/FieldLabelAndInfo/index.tsx passes the description string to React's dangerouslySetInnerHTML, and no layer between storage and render escapes or sanitises it; the neighbouring info values in the same component are rendered as React children and are escaped, so the description is the only raw path. A description is free-form text held in the dataset schema, so it persists in the database and travels with an exported or published dataset. Opening a dataset obtained from another party and hovering the field runs the stored markup in the application's origin. That origin is shared with the FiftyOne server, whose media route returns the contents of a caller-named absolute path and which is unauthenticated in the open-source server, so the injected script can read local files and reach the dataset and operator endpoints as the viewing user.	7.1	More Details
CVE-2026-78281	Unauthenticated Cross Site Scripting (XSS) in CP Media Player <= 1.3.0 versions.	7.1	More Details
CVE-2026-78283	Unauthenticated Cross Site Scripting (XSS) in Music Player for WooCommerce <= 1.8.9 versions.	7.1	More Details
CVE-2025-29419	CTFd v3.7.6 was discovered to be vulnerable to a man-in-the-middle attack.	7.1	More Details
CVE-2026-78289	Unauthenticated Cross Site Scripting (XSS) in CozyStay <= 1.10.0 versions.	7.1	More Details
CVE-2026-47849	Spring Data REST does not guard identifier (@Id) and version (@Version) properties against mutation via RFC 6902 JSON Patch (application/json-patch+json) requests. Spring Data REST 5.1.0 Spring Data REST 5.0.0 - 5.0.6 Spring Data REST 4.5.0 - 4.5.12 Spring Data REST 4.0.0 - 4.4.15 Spring Data REST 3.7.20 and earlier	7.1	More Details
CVE-2026-80530	In the Linux kernel, the following vulnerability has been resolved: xfs: fix exchange-range reflink flag clearing issue with INO1_WRITTEN When exchanging two full-file ranges, xmi_can_exchange_reflink_flags() can move the reflink inode flag from the file that currently has it to the other file, as long as exactly one side is marked. This assumes that the file contents, and therefore all shared extents, are exchanged. That assumption is not true when XFS_EXCHMAPS_INO1_WRITTEN is set. xfs_exchmaps_can_skip_mapping() can skip hole and unwritten mappings from file1, so an exchange can complete without moving every mapping that the earlier flag-swap decision accounted for. In that case the post-operation cleanup can clear the reflink flag from an inode that still owns shared written extents. Later writes then take the non-reflink write path and may update blocks that should still have been protected by CoW, which shows up as data corruption between reflink-related files. Fix this by disabling the reflink flag exchange whenever XFS_EXCHMAPS_INO1_WRITTEN is requested. The contents exchange can still proceed; the conservative outcome is that both inodes keep the reflink flag. The regular reflink flag cleanup path can drop the extra flag later once the inode no longer has shared extents.	7.1	More Details
CVE-2026-78293	Unauthenticated Cross Site Scripting (XSS) in WP w3all phpBB <= 3.0.6 versions.	7.1	More Details
CVE-2026-80350	OneUptime's webhook target check rejects private and loopback addresses given in IPv4 form and a small set of IPv6 forms, but has no case for the IPv4-mapped IPv6 range. The webhook delivery path calls SSRFProtection.validateWebhookTargetIsSafe, and the host-literal screening inside Common/Server/Utils/SSRFProtection.ts, performed by isBlockedHostnameLiteral, rejects private and loopback IPv4 ranges and tests an IPv6 value against the unspecified address, the loopback, the link-local prefix and the unique-local prefixes. A value such as [::ffff:127.0.0.1] matches none of them. The value is also recognised as an address literal rather than a name, so the path that re-checks addresses obtained from resolution is not taken. The HTTP client treats the mapped form as the embedded IPv4 address and connects to it, so an authenticated project member who can configure a webhook can direct the server at loopback services, private network ranges and link-local metadata endpoints, and the response is recorded where the webhook result can be read. Version 12.0.7 adds handling for the mapped range.	7.1	More Details
CVE-2026-80346	StarRocks performs no privilege check when a legacy synchronous materialized view is dropped. Every other statement type routed through AuthorizerStmtVisitor calls into Authorizer before execution, but visitDropMaterializedViewStatement returns immediately with a comment stating the check happens in execution logic. That holds only for asynchronous materialized views: LocalMetastore.dropMaterializedView calls Authorizer.checkMaterializedViewAction inside a branch taken when the resolved table is a MaterializedView. A legacy synchronous materialized view is stored as a rollup index on an OlapTable rather than a MaterializedView, so the other branch runs, reaching AlterJobMgr.processDropMaterializedView and MaterializedViewHandler, neither of which contains any Authorizer call. The former locates the target by scanning every OlapTable in the named database for a matching rollup index, and the latter validates only	7.1	More Details

	table state and name conflicts. Any authenticated account can therefore drop a legacy synchronous materialized view belonging to any database, holding no grant on the view, the base table or the database, and the drop is indistinguishable from an authorized one.		
CVE-2026-80555	In the Linux kernel, the following vulnerability has been resolved: s390/vfio_ccw: Free all memory if cp_init() fails The routine cp_free() is called to unpin/free any memory once an I/O is completed successfully, or if cp_prefetch() fails. But if cp_init() fails, and cp->initialized is not enabled, the same routine cannot be used to free all the memory. An attempt to address this exists in ccwchain_handle_ccw(), where a single call to ccwchain_free() is made for the currently-processed CCW segment. But this will leak other segments (created as a result of a Transfer in Channel) that had been allocated as part of the same channel program. Address this by performing the cleanup outside of the recursive ccwchain_handle_ccw()/ccwchain_loop_tic() logic.	7.1	More Details
CVE-2026-77611	SeaweedFS is a distributed storage system for files and blobs. In versions prior to 4.40, an authenticated S3 principal with permissions scoped to a nested object key can overwrite a different object outside that scope by calling PutObjectAcl on the key it is allowed to access. The handler authorizes the request against the requested nested key but then writes the updated entry back to the bucket root rather than the key's actual parent directory, so an ACL change on allowed/protected.txt is instead applied to protected.txt at the bucket root. Because the update carries the full entry rather than only ACL metadata, an existing target object is overwritten with the content, metadata, owner information, and ACL of the scoped object, bypassing the object-level action scoping configured through the static S3 identity file. This issue is fixed in version 4.40.	7.1	More Details
CVE-2026-81726	NLTK through 3.10.3 contains a path traversal vulnerability in model-artifact APIs that bypass pathsec enforcement by using raw file operations on caller-controlled paths. Attackers can read or write files outside allowed sandbox roots through TransitionParser, AveragedPerceptron, PerceptronTagger, and maxent parameter APIs when pathsec is enabled.	7.0	More Details
CVE-2026-16821	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to gain elevated privileges due to a format string vulnerability.	7.0	More Details
CVE-2026-81714	openssl_encrypt (pip: openssl-encrypt) versions <= 1.4.8 use suffix-tolerant fingerprint matching in enroll_trust_key when binding a plugin-signing trust anchor. An operator who confirms a short (forgeable, ~32-bit) GPG key id could unknowingly enroll an attacker's colliding key as a trusted anchor, which then vouches for malicious plugins under the ENFORCE signature policy. Version 1.4.9 fixes this by requiring the confirmed value to exactly match the full primary-key fingerprint (case-insensitive, whitespace-stripped).	7.0	More Details
CVE-2026-54467	On the Trusted Firmware-M (TF-M) 2 through 2.3.0 platform before 00d1b3e, mailbox initialization on PSOC64 and RP2350 accepts a non-secure, unvalidated, supplied pointer.	7.0	More Details
CVE-2026-58093	The TIOCSCTTY ioctl handler drops the tty lock in order to acquire the process tree lock. After reacquiring the tty lock, the handler did not revalidate the state of the terminal, and could proceed to link a terminal that was concurrently being destroyed to the calling process' session. An unprivileged local user can exploit this race condition to escalate privileges.	7.0	More Details
CVE-2026-59311	A local unprivileged user on the same host can redirect all Zip/UnZip transformer output into a directory of their choosing by pre-creating /tmp/ziptransformer as a symlink before the application starts. Spring Integration 7.1.0 Spring Integration 7.0.0 - 7.0.5 Spring Integration 6.5.0 - 6.5.10 Spring Integration 6.4.0 - 6.4.12	6.8	More Details
CVE-2026-78275	Editor Arbitrary File Deletion in Fluent Boards Pro <= 2.0.11 versions.	6.8	More Details
CVE-2026-82020	Hermes Agent 0.16.0 prior to 0.17.0 contains an improper path restriction vulnerability that allows attackers who can influence ingested message content to overwrite the credential store by bypassing sensitive-path guards that excluded the auth.json file. Attackers can craft malicious messages directing the agent's file-write tooling to overwrite the credential store without triggering any path-based protection, enabling credential tampering or unauthorized access.	6.8	More Details
CVE-2026-82262	Logto through 1.42.0 contains a server-side request forgery vulnerability in the POST /api/hooks/:id/test endpoint that accepts arbitrary URLs without host validation. Tenant administrators with Management API tokens can make the server issue HTTP POST requests to internal URLs and retrieve response bodies from services on the private network.	6.8	More Details
CVE-2026-82263	Logto through 1.42.0 contains a server-side request forgery vulnerability in the OIDC SSO connector creation endpoint that fails to validate the issuer URL parameter. Tenant administrators with Management API credentials can supply arbitrary internal URLs to trigger HTTP GET requests to private network services, with response content returned in API responses.	6.8	More Details
CVE-2026-82264	Duplicacy through 3.2.5 contains a path traversal vulnerability in the restore function that fails to validate entry paths deserialized from snapshot files. Attackers can craft malicious snapshot entries with directory traversal sequences to write files outside the restore directory to arbitrary locations accessible by the restoring user.	6.8	More Details
	The SOGO Add Script to Individual Pages Header Footer WordPress plugin through 3.9 does not sanitise or		

CVE-2026-14835	escape the custom header/footer script values saved from its post metabox, and does not restrict them to users with the unfiltered_html capability, allowing users with contributor-level access and above to store JavaScript that executes in the browser of any administrator who reviews the post and of any visitor once the post is published.	6.8	More Details
CVE-2026-19226	The Royal Addons for Elementor WordPress plugin before 1.7.1066 does not validate some widget settings before outputting them inside an HTML attribute, which could allow users with the Contributor role and above to perform Stored Cross-Site Scripting attacks.	6.8	More Details
CVE-2026-32639	Winter CMS is a content management system built on the Laravel PHP framework. In versions up to and including 1.2.12, the CMS section's Theme Editor AJAX handlers did not enforce per-template-type permission checks, allowing a backend user with any single CMS permission to act on template types outside their authorized scope. The CMS controller gated access to the section as a whole using OR-logic across its five permissions, but individual handlers such as onSave(), onDelete(), and onDeleteTemplates() did not verify that the user held the specific permission for the requested template type, so a user with only cms.manage_pages could craft AJAX requests to delete layouts, modify partials, or read content files. Separately, the AssetList widget was registered for any user who passed the controller gate regardless of the cms.manage_assets permission, and its onUpload() handler omitted the theme-validation call present on the other mutating handlers, permitting unauthorized file uploads into the active theme's asset directory. Exploitation requires an authenticated backend account holding at least one of the CMS Theme Editor permissions. This issue is fixed in version 1.2.13.	6.8	More Details
CVE-2026-47837	Missing Authentication for Critical Function vulnerability in Spring Spring Cloud Config allows Webhook requests to Spring Cloud Config Server's /monitor endpoint are not validated. This issue affects Spring Cloud Config: from 5.0.0 through 5.0.4, from 4.3.0 through 4.3.4, from 4.0.0 through 4.2.8, and through 3.1.14.	6.8	More Details
CVE-2026-81706	openssl_encrypt before 1.4.9 fails to prevent namespace collisions between own identities and contacts in IdentityStore, allowing attackers to create shadowed contact entries invisible until the corresponding own identity is deleted. When the own identity is deleted, the shadowed contact becomes visible and resolves to the attacker's keys, enabling silent key substitution for encrypted files.	6.8	More Details
CVE-2026-82866	@pdfme/common before 5.5.10 contains a server-side request forgery vulnerability in the getB64BasePdf function that fetches arbitrary URLs without validation when basePdf is attacker-controlled. Attackers who control the basePdf template field can force servers or clients to make requests to internal endpoints, enabling metadata exfiltration, network reconnaissance, and blind request forgery attacks.	6.8	More Details
CVE-2026-75364	Comfast CF-N1-S firmware 2.6.0.1 and CF-WR630AX (2024-01-30 build), the update_interface_png SET handler in /usr/bin/webmgnt fails to sanitize the display_name parameter. User-controlled input is concatenated via sprintf() into the unquoted shell command `/etc/rrd/graphinterface %s %s` and executed by system() with root privileges. A remote authenticated attacker can inject arbitrary commands	6.8	More Details
CVE-2026-75363	An issue in Comfast CF-WR630AX v.2.7.0.2 allows a remote attacker to execute arbitrary code via the /usr/bin/webmgnt, /cgi-bin/mbox-config, and the parameters timestr, display_n.	6.8	More Details
CVE-2026-81100	tiger-gh-mcp-server started its MCP HTTP transport without enabling the host allow-list the underlying SDK provides. src/httpServer.ts called the shared httpServerFactory helper and never set the DNS-rebinding-protection option, so the transport accepted a request whatever host it named, making the locally reachable GitHub MCP endpoint drivable from a page in a visitor's browser that pointed a name it controlled at the bound address. The fix passes the option explicitly alongside a dependency update; the update alone would not have closed it. The repository has published no release that brackets the fix, so the affected boundary is the commit preceding it.	6.8	More Details
CVE-2026-81099	tiger-slack started its MCP HTTP transport without enabling the host allow-list the underlying SDK provides. mcp/src/httpServer.ts called the shared httpServerFactory helper and never set the DNS-rebinding-protection option, so the transport accepted a request whatever host it named, and a page in a browser could point a name it controlled at the address the server was bound to and drive the locally reachable Slack MCP server through the visitor's browser. The fix passes the option explicitly alongside a dependency update; the update alone would not have closed it. The repository publishes no release that brackets the fix, so the affected boundary is the commit preceding it.	6.8	More Details
CVE-2026-12513	The Shared Files WordPress plugin before 1.7.67, shared-files-pro WordPress plugin before 1.7.68 do not properly sanitize a file path taken from a frontend file submission and their single-pass traversal filter is bypassable, allowing unauthenticated users to store a path that points outside the uploads directory. When the corresponding file entry is later permanently deleted, an arbitrary file on the server (such as wp-config.php) is deleted, leading to denial of service and potential site takeover.	6.8	More Details
CVE-2026-81095	pg-aiguide started its MCP HTTP transport without enabling the host allow-list the underlying SDK provides. src/httpServer.ts called the shared httpServerFactory helper and never set the DNS-rebinding-protection option, so the transport accepted a request whatever host it named. A page in a browser could therefore point a name it controlled at the address the server was bound to and drive the locally reachable MCP server through the visitor's browser. The protection was already available in the packaged transport and simply not turned on, so updating the dependency alone would not have closed it. Version 0.5.1 passes the option explicitly.	6.8	More Details

CVE-2026-81092	mcp-go accepted requests on its HTTP transports without checking the Host header. StreamableHTTPServer.ServeHTTP in server/streamable_http.go and SSEServer.ServeHTTP in server/sse.go served any request arriving over a loopback connection regardless of the host it named, and the SSE transport's cross-origin default allowed any origin. A page in a browser could therefore point a name it controlled at the loopback address and reach a server listening there, invoking tools and reading resources that the server exposed on the assumption that only local software could connect. No release before 0.56.0 validated the header on either transport; 0.56.0 adds server/http_localhost.go, which rejects a loopback-bound request carrying a host that is not a loopback name, and wires it into both transports.	6.8	More Details
CVE-2026-76546	The User Profile Builder WordPress plugin before 4.0.1 does not escape the output of one of its optional shortcodes, allowing users with a role as low as contributor to perform Stored Cross-Site Scripting attacks against any user viewing the affected content, including administrators. The shortcode is not enabled by default.	6.8	More Details
CVE-2026-59272	Any application shipping logs to RabbitMQ over TLS via the Log4j2 appender, relying on the documented default, is exposed to man-in-the-middle interception of every log event. Spring AMQP 4.1.0 Spring AMQP 4.0.0 - 4.0.4 Spring AMQP 3.2.0 - 3.2.12 Spring AMQP 2.4.18 and earlier	6.8	More Details
CVE-2026-82255	gitoxide versions from 0.25.4 contain an HTTP credential leak vulnerability in the curl-based transport backend where credentials are sent to attacker-controlled servers after HTTP redirects. The vulnerability occurs because credential validation checks the original URL instead of the effective URL after redirect, allowing attackers to steal authentication tokens through cross-domain redirects or HTTPS-to-HTTP downgrades.	6.8	More Details
CVE-2026-82702	A vulnerability was identified in Edimax BR-6214K 1.40. This affects the function system of the file www/wlanMP.asp of the component asp_WlanMP Endpoint. Such manipulation of the argument ateFunc leads to os command injection. It is possible to launch the attack remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.6	More Details
CVE-2026-82703	A security flaw has been discovered in Edimax BR-6214K 1.40. This vulnerability affects the function system of the file www/ping.asp of the component asp_setPing Endpoint. Performing a manipulation of the argument pingstr results in os command injection. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	6.6	More Details
CVE-2026-81766	The Really Simple Security WordPress plugin before 9.8.0 does not check that the user is allowed to install Really Simple Security WordPress plugin before 9.8.0 before installing one from a user-supplied URL, allowing an administrator of a subsite on a multisite network to install and execute arbitrary code in the network-shared Really Simple Security WordPress plugin before 9.8.0 directory, which WordPress otherwise reserves to the network administrator. Exploitation requires the network administrator to have enabled the Really Simple Security WordPress plugin before 9.8.0 administration menu for subsites, which is not the default.	6.6	More Details
CVE-2026-19225	The Defender Security WordPress plugin before 6.2.0 does not restrict a network-wide setting to network administrators, allowing an administrator of any single site on a multisite network to execute arbitrary code across the entire network.	6.6	More Details
CVE-2026-59275	A single hostile AMQP message can terminate the entire consumer JVM (System.exit(99)), not just the listener thread — full availability loss for every workload co-located in that process. Spring AMQP 4.1.0 Spring AMQP 4.0.0 - 4.0.4 Spring AMQP 3.2.0 - 3.2.12 Spring AMQP 2.4.18 and earlier	6.6	More Details
CVE-2026-59293	Unless the application explicitly raises smbMinVersion, the jCIFS client will negotiate down to SMB1/CIFS, which lacks mandatory signing/encryption and is vulnerable to NTLM relay and content-tampering MITM. Spring Integration 7.1.0 Spring Integration 7.0.0 - 7.0.5 Spring Integration 6.5.0 - 6.5.10 Spring Integration 6.4.0 - 6.4.12	6.6	More Details
CVE-2026-76547	The User Profile Builder WordPress plugin before 4.0.1 does not validate the type of data being deserialized when importing a configuration file, allowing high privilege users such as administrators to conduct PHP Object Injection. The affected feature is a free add-on which is disabled by default, and no POP chain is present in the User Profile Builder WordPress plugin before 4.0.1 itself, so further impact requires a suitable gadget from another installed User Profile Builder WordPress plugin before 4.0.1 or .	6.6	More Details
CVE-2026-55569	aqua is a declarative command-line version manager written in Go. Prior to 2.60.1, pkg/unarchive/archives.go in the handler.HandleFile method calls os.Symlink with archives.FileInfo.LinkTarget without verifying that the target remains under the extraction destination. A later regular-file entry at the same archive path is opened with OpenFile using O_CREATE and O_WRONLY, which follows the attacker-planted symlink. A malicious or compromised package archive can therefore write attacker-controlled bytes outside aqua's extraction directory with the privileges of the user running aqua, potentially overwriting shell startup files, tool configuration, or writable executable paths. This issue is fixed in version 2.60.1.	6.6	More Details
CVE-2026-74771	Dell PowerProtect One, versions 20.1.0.0 and below, contain an Authorization Bypass Through User-Controlled Key vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Information tampering.	6.5	More Details

CVE-2026-16759	The Tutor LMS – eLearning and online course solution plugin for WordPress is vulnerable to Remote Code Execution limited to zero-argument function invocation in all versions up to, and including, 4.0.5 via the tutor_course_filter_ajax AJAX action. This is due to missing authorization on the handler combined with unsanitized array keys being passed to extract() inside tutor_load_template(), allowing attacker-controlled POST data to overwrite the local $template variable and, in the resulting templates/single-content-loader.php template, the $method_map and $context variables invoked at $method_map[$context](). This makes it possible for unauthenticated attackers to call an arbitrary zero-argument PHP function server-side and, via WordPress core edit_user(), to create a persistent subscriber-level account from request parameters.	6.5	More Details
CVE-2026-78146	The Simple Newsletter Plugin WordPress plugin before 4.3.3 does not verify that the requester is the subscriber named in a public request before rendering that subscriber's stored details, allowing unauthenticated users to disclose a subscriber's personal data along with the key that authorises changes to their record.	6.5	More Details
CVE-2026-66324	External control of file name or path in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	6.5	More Details
CVE-2026-61802	Wazuh is an open-source security platform providing unified XDR and SIEM protection for endpoints and cloud workloads. In versions 4.14.0 through 4.14.6, a low-privilege API user can read the cleartext cluster key from a configuration endpoint that fails to redact it. The REST API provides a masking control, mask_sensitive_config, that redacts sensitive fields such as authd.pass and cluster.key from configuration responses for users who lack update-config permission, and every config-read endpoint carries this decorator except GET /cluster/local/config. That endpoint, backed by read_config_wrapper, is gated only by cluster:read and returns the local node's cluster configuration including the cleartext key, whereas its siblings return the same value masked. As a result, any account with the default readonly or cluster_readonly role, which is explicitly denied update-config precisely so it cannot view secrets, receives the real cluster key. Because the cluster key authenticates and encrypts traffic between cluster nodes, disclosing it to an unprivileged account provides the authentication precondition for the cluster-peer remote code execution chains established by prior advisories. This issue is fixed in version 4.14.	6.5	More Details
CVE-2026-62326	Weblate is a web-based continuous localization platform used to manage software translations. In versions prior to 2026.7, a user with the built-in "Edit source" role can store a malicious regular expression in a source string's flags that is executed without any timeout, allowing them to stall requests and deny service. Regular expressions supplied through the regex: quality check and regex placeholders are compiled during validation but later run against translation content in RegexCheck and PlaceholderCheck with no time limit, so a catastrophic-backtracking pattern like ^(a|aa)+$ can consume CPU indefinitely. Because Weblate re-runs these checks for every linked target unit in the same request when a source unit's flags change, a single edit can trigger sustained CPU-bound denial of service. This issue is fixed in version 2026.7.	6.5	More Details
CVE-2026-37009	A SQL injection vulnerability in NL2SQLTool in crewai-tools v1.10.2rc1 allows a remote attacker to execute arbitrary SQL commands via an unsanitized sql_query argument.	6.5	More Details
CVE-2026-68967	Bendix EC80 Brake ECU is vulnerable to an out-of-bounds write, which could allow an attacker to deliver a payload that could establish an arbitrary write primitive, which could crash the ECU.	6.5	More Details
CVE-2026-75132	WAPT Server versions 2.6.1.17834 and earlier contains a SQL injection vulnerability in the `columns` parameter of the GET `/api/v3/hosts` endpoint. A remote authenticated user with read-only privileges can inject arbitrary PostgreSQL expressions into the SQL query constructed by WAPT. By exploiting the injection point, an attacker can inject additional PostgreSQL statements, bypass the host scope restrictions applied to the account, and read information from other rows or tables within the database.	6.5	More Details
CVE-2026-82306	StarRocks through 4.0.13 contains an information disclosure vulnerability in the query_detail endpoint that returns unfiltered query history for all users. Authenticated attackers with low privileges can access full SQL text, execution plans, and profiling data from every query executed by other users, including statements containing credentials.	6.5	More Details
CVE-2026-77975	The affected Ebyte product exports administrative credentials and other sensitive configuration information without adequate protection. An unauthenticated attacker on the adjacent network who can obtain an exported configuration file could recover valid credentials and use them to access the device or similarly configured systems.	6.5	More Details
CVE-2026-82877	ILIAS versions before 9.22, 10.0 through 10.9, and 11.0 through 11.2 contain an arbitrary file read vulnerability in the SOAP addFile method that allows authenticated users to read server files by supplying crafted XML with COPY-mode imports. Attackers can construct absolute file paths through an unsandboxed import directory and retrieve sensitive files including configuration files containing database credentials and setup passwords.	6.5	More Details
CVE-2026-78273	Subscriber Cross Site Scripting (XSS) in Fluent Boards Pro <= 2.0.11 versions.	6.5	More Details
CVE-2026-	When Apache Shiro is used with the Jakarta EE integration module, a low-privileged user can craft an HTTP request that causes the server to initiate a connection to an attacker-controlled URL and transmit attacker-controlled data. This vulnerability affects Apache Shiro versions 2.x through 3.0.0 only in deployments that use the Jakarta EE integration module. Mitigation: Upgrade to version 3.0.1 or later, which fixes the issue. +	6.5	More

58301	Alternatively, you can set the `org.apache.shiro.form-resubmit-host` (String) and `org.apache.shiro.form-resubmit-port` (Integer) system properties to restrict the host and port that Shiro will connect to when resubmitting a form.		Details
CVE-2026-13734	Zephyr's WireGuard VPN data-plane receive handler wg_process_data_message() in subsys/net/lib/wireguard/wg_crypto.c validated the anti-replay counter too late. After AEAD decryption of a MESSAGE_TRANSPORT_DATA packet succeeded, the code committed several peer-state changes — update_peer_addr() (endpoint roaming update), the keypair->last_rx/peer->last_rx liveness timers, and keypair_update() (promote next→current and destroy the previous keypair) — and only afterward called wg_check_replay(). On a replayed packet the replay check returned -EINVAL, but none of the preceding mutations were rolled back. The AEAD tag authenticates content but not freshness, so a replayed-but-authentic transport packet decrypts correctly. An attacker who captures one valid ciphertext off the wire (an on-path or shared-medium observer) can re-inject it from an arbitrary spoofed source address. Reaching the handler requires no credentials: it is driven directly from inbound UDP datagrams via the dispatch in subsys/net/lib/wireguard/wg.c. Because the state mutations committed before the replay check, the replay repoints the peer endpoint to the attacker-chosen source address (roaming hijack), redirecting the victim's subsequent outbound tunnel traffic until the legitimate peer's next packet re-corrects it; it also prematurely destroys the previous keypair and refreshes the RX liveness timer. The tunnel payload stays encrypted under the session keypair, so this is an integrity/availability impact (traffic redirection and session disruption), not payload disclosure. The fix moves wg_check_replay() to immediately after a successful decrypt, before any peer-state mutation, matching the WireGuard specification and the Linux reference implementation.	6.5	More Details
CVE-2026-16984	The Privacy Policy Generator, Terms & Conditions, GDPR, CCPA, Cookie Policy & Disclaimer Templates WordPress plugin before 3.7.1 does not include an authorization check on a REST route that returns stored account data, allowing unauthenticated visitors to retrieve the connected service's API secret and account details, which can then be used to disconnect the Privacy Policy Generator, Terms & Conditions, GDPR, CCPA, Cookie Policy & Disclaimer Templates WordPress plugin before 3.7.1's integration.	6.5	More Details
CVE-2025-70340	A Broken Access Control vulnerability exists in ThingsBoard Professional Edition (PE) 4.21 and below, within the Alarms comments functionality. An authenticated customer user can manipulate the respective API request parameters to create or modify system-generated alarm comments. This allows unauthorized impersonation of system messages and modification of trusted system-owned data, resulting in vertical privilege escalation and potential integrity violations.	6.5	More Details
CVE-2026-75466	libjpeg-turbo 3.2.0 contains an integer division-by-zero vulnerability in the PNG loader. When processing a valid indexed-color PNG image with a non-gray palette through tj3LoadImage12() or tj3LoadImage16() using the default pixel format, the application may trigger a division-by-zero in alloc_sarray(), causing a SIGFPE and denial of service.	6.5	More Details
CVE-2026-55549	Yamcs is a mission control framework. Prior to 5.9.4, Yamcs reflects an attacker-controlled redirect_uri parameter from GET /auth/authorize into yamcs-core/src/main/resources/auth/templates/authorize.html without adequate HTML escaping by yamcs-core/src/main/java/org/yamcs/http/auth/AuthHandler.java and yamcs-core/src/main/java/org/yamcs/http/HandlerContext.java. A crafted authorization URL can execute JavaScript when opened by a Yamcs user. The script can access browser-held authentication material and transmit it to an attacker, enabling account compromise. This issue is fixed in version 5.9.4.	6.5	More Details
CVE-2026-82864	pdfme pdf-lib versions before 5.5.10 contain an unbounded buffer growth vulnerability in the DecodeStream.ensureBuffer() method that allows attackers to cause denial of service by supplying a crafted PDF with a FlateDecode stream containing a decompression bomb. Attackers can upload a small compressed PDF that decompresses to hundreds of megabytes, exhausting memory and crashing the Node.js process or freezing browser tabs during PDF parsing.	6.5	More Details
CVE-2026-82662	Nodemailer before 8.0.8 disables TLS certificate verification in lib/fetch/index.js through rejectUnauthorized: false, allowing attackers to intercept OAuth2 token requests. Attackers in a machine-in-the-middle position can capture OAuth client secrets, refresh tokens, and access tokens transmitted over compromised HTTPS connections.	6.5	More Details
CVE-2026-19953	URI versions before 5.36 for Perl encode non-NFC host names to non-standard punycode labels via missing normalization in nameprep. nameprep lowercases each host label but performs no Unicode normalization. IDNA requires a label to be normalized to Form C before it is encoded (RFC 5891), so a label that is not already in NFC is encoded to a different A-label than its normalized form. A label built from the precomposed Devanagari sequence U+0958 U+093E encodes to xn--72b5c without normalization but to xn--11b2fg after NFC normalization, and xn--72b5c does not round-trip back to the original label. Any caller that reads host() from a URI built from untrusted input and uses it for a security decision (an allow or deny list, an SSRF filter, deduplication, a cache key) sees the non-standard label, while a client that fetches the same URL resolves the NFC form, so the check and the fetch can disagree about the host.	6.5	More Details
CVE-2026-	Fleet is an open-source device management platform built on osquery. In versions prior to 4.87.0, the target search endpoint (POST /api/latest/fleet/targets) returned unmasked team enroll secrets and full team configuration, including credential-bearing agent options, to low-privilege observer-class users. Other team-facing endpoints mask these fields for observers, but the target search endpoint did not apply the same sanitization, so an authenticated user with the Observer, Observer+, or Technician role, whether global or	6.5	More

48786	team-scoped, could retrieve the secrets and agent options by performing a target search against an observer-runnable query. With a leaked team enroll secret an attacker could enroll unauthorized hosts into the affected team, and if the team's agent options contained credentials such as AWS secret access keys or proxy passwords, those values were disclosed as well. This issue is fixed in version 4.87.0.		Details
CVE-2026-38343	An integer overflow in the libavfilter/vf_scale.c component of FFmpeg N-122528-gdd2976b9e1 allows attackers to cause a Denial of Service (DoS) via supplying a crafted video file.	6.5	More Details
CVE-2026-46370	Fleet is an open-source device management platform built on osquery. In versions up to and including 4.84.1, the labels host-listing endpoint (GET /api/v1/fleet/labels/{id}/hosts) allowed an authenticated user with the lowest-privilege Observer role to extract host enrollment secrets through a sort-order oracle. The endpoint accepted a user-supplied order_key parameter that was not validated against a column allowlist, so an attacker with Global or Team Observer access could set the sort column to a sensitive field such as h.node_key and combine it with the cursor-based after parameter to binary-search the value one character at a time; the targeted value never appeared in the response, but the presence or absence of results revealed each character. Because node_key and orbit_node_key are the long-lived shared secrets that osquery and Orbit agents use to authenticate to the Fleet server, an attacker who reconstructed them could impersonate enrolled hosts, submit fabricated query results and inventory, retrieve pending scripts and MDM commands, and poison compliance and policy results across the deployment. This issue is fixed in version 4.84.2.	6.5	More Details
CVE-2026-82271	R2R through 3.6.5 fails to properly validate user ownership in conversation update and message handlers, allowing authenticated users to modify other users' conversations. Attackers can supply arbitrary conversation identifiers to rename conversations and append messages to other users' conversation histories, corrupting state and injecting malicious content.	6.5	More Details
CVE-2026-46371	Fleet is an open-source device management platform built on osquery. In versions up to and including 4.84.1, the Apple MDM commands listing endpoint (GET /api/v1/fleet/mdm/apple/commands) allowed an authenticated user with the lowest-privilege Observer role to extract sensitive values from joined database tables, including host enrollment secrets and Apple Push Notification Service tokens, through a sort-order oracle. The endpoint accepted a user-supplied order_key parameter that was not validated against a column allowlist, and because the underlying query joins the hosts and nano_enrollments tables, an attacker could set the sort column to a sensitive field and combine it with the cursor-based after parameter to binary-search the value one character at a time, with the presence or absence of results revealing each character even though the value never appeared in the response. With extracted node_key or orbit_node_key values an attacker could impersonate enrolled hosts to Fleet's osquery and Orbit endpoints, submit fabricated host data, and retrieve pending scripts and commands. This issue is fixed in version 4.84.2.	6.5	More Details
CVE-2026-14216	The Booking for Appointments and Events Calendar WordPress plugin before 2.4.7 does not require authentication before processing its pending notification queue, allowing an unauthenticated user to force the dispatch of queued notifications and integration callbacks.	6.5	More Details
CVE-2026-82272	Immich through 3.1.0 fails to properly enforce locked asset visibility when assets are locked through the single-asset endpoint, allowing them to remain accessible through shared albums and links. Attackers can read locked assets and their metadata by accessing existing shared albums or links, bypassing the locked visibility protection.	6.5	More Details
CVE-2026-82273	Mastra through 1.63.0 contains an authentication bypass vulnerability in the memory API thread ownership validation when mapUserToResourceId callback is omitted from configuration. Authenticated attackers can enumerate all threads via GET /api/memory/threads and read conversation history and metadata of other resource owners.	6.5	More Details
CVE-2026-82265	Zipkin through 3.6.1 exposes Spring Boot Actuator endpoints on the tracing API port without authentication, allowing unauthenticated attackers to access sensitive information. Attackers can read environment variables, bean configurations, and storage credentials via actuator endpoints, or modify log levels to suppress logging.	6.5	More Details
CVE-2026-71054	Vulnerability in Oracle Java SE (component: 2D). Supported versions that are affected are Oracle Java SE: 7u511. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Java SE. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L).	6.5	More Details
CVE-2026-81341	wolfEngine before 1.4.1 sources the explicit AES-CCM nonce for TLS 1.2 and DTLS 1.2 records from the record input buffer instead of the TLS sequence number carried in the additional authenticated data. Because the record layer leaves the explicit-nonce field for the cipher to populate, the value read is constant across records, so every AES-CCM record within a connection is encrypted under an identical key and nonce pair. Reusing a CCM key and nonce weakens confidentiality (identical keystream across records, so a known record recovers the others) and integrity (authentication tag forgery). Only wolfEngine is affected;	6.5	More Details

	wolfProvider is not. AES-GCM under wolfEngine is tracked separately. AES-CCM cipher suites are not enabled by default and must be explicitly selected, which limits exposure. TLS 1.3 and non-TLS use of the cipher are not affected.		
CVE-2026-77695	The Return Refund and Exchange For WooCommerce WordPress plugin before 4.6.4 does not correctly verify the ownership of guest orders in some of the AJAX actions it exposes to unauthenticated users, allowing them to read private order messages, post messages and attachments in the customer's name, and cancel return requests on any guest order.	6.5	More Details
CVE-2026-47860	An attacker who can publish to a queue consumed by an application that has enabled message decompression can crash the consumer JVM with a single ~1 MB message. Spring AMQP 4.1.0 Spring AMQP 4.0.0 - 4.0.4 Spring AMQP 3.2.0 - 3.2.12 Spring AMQP 2.4.18 and earlier	6.5	More Details
CVE-2026-54732	libreoffice-convert is a Node.js module for converting office documents to different formats. Prior to 1.8.2, index.js uses the caller-controlled options.fileName value in path.join(tempDir.name, fileName) without reducing it to a base name. A filename containing ../ can escape the temporary directory because path.basename() normalization is missing and write the supplied document buffer to an arbitrary path writable by the process, including an SSH authorized_keys file, a cron configuration, or a web root. This issue is fixed in version 1.8.2.	6.5	More Details
CVE-2026-77939	Flextype CMS through v1.0.0-dev contains an expression language injection vulnerability that allows authenticated attackers with a valid API token to read arbitrary files by passing unsanitized user-supplied input to the Symfony ExpressionLanguage engine via the POST /api/v1/query endpoint. Attackers can leverage exposed application objects including filesystem() and serializers() within the evaluation scope to read arbitrary server files and achieve conditional remote code execution if a PHP file can be placed on disk through a secondary vector.	6.5	More Details
CVE-2026-17562	Authorization bypass through User-Controlled key vulnerability in Summit Security Systems AdisyonPro allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects AdisyonPro: before v5.21.0.	6.5	More Details
CVE-2026-59317	DeadLetterPublishingRecovererFactory reads the retry_topic-original-timestamp header from an inbound ConsumerRecord and passes its raw bytes directly to new BigInteger(header.value()) with no length or format validation. Spring for Apache Kafka 4.1.0 Spring for Apache Kafka 4.0.0 - 4.0.6 Spring for Apache Kafka 3.0.0 - 3.3.16 Spring for Apache Kafka 2.9.0 - 2.9.14 Spring for Apache Kafka 2.8.12 and earlier	6.5	More Details
CVE-2026-49809	Dell PowerProtect Cyber Recovery, versions 20.2 and prior, 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.	6.5	More Details
CVE-2026-59320	When a container-level ErrorHandler is configured (the mitigation for finding 221000), each delivery whose processing throws still permanently consumes one link credit. After initialCredits (default 100) failing messages the receiver's credit reaches zero and the broker stops delivering, leaving the listener silently stalled while isRunning() remains true. Spring AMQP 4.1.0	6.5	More Details
CVE-2026-81658	A flaw was found in Foreman. The template revision endpoint does not enforce object-level authorization when retrieving an audited template revision. An authenticated, low privileged user with a template-related permission, such as view_ptables, can obtain historical template contents belonging to another organization or location by supplying the corresponding audit ID. This can result in unauthorized disclosure of historical template contents, which may contain sensitive configuration information, credentials, or other secrets. The REST API revision endpoints correctly restrict this lookup.	6.5	More Details
CVE-2026-51376	An issue in BitChat for iOS v1.15.0 allows a remote attacker to cause a denial of service via an unauthenticated MESSAGE packet into the mesh gossip cache	6.5	More Details
CVE-2026-81521	The MongoDB Go Driver's client-level bulk write operation may accept a caller-supplied database name containing a reserved separator character without escaping it before the name is used to build the target namespace for the operation. An application that passes untrusted input as a database name could therefore have the write directed at a database and collection other than the ones it intended. Only the Client.BulkWrite API is affected.	6.5	More Details
CVE-2026-81526	The MongoDB Rust Driver does not neutralize special characters in a caller-supplied target identifier before embedding it in the request it sends to the server. An actor able to influence that identifier in an application using the driver may cause write operations to be applied to an unintended target within the same deployment using the application's own credentials. This may result in unauthorized modification of data belonging to another logical boundary enforced by the application.	6.5	More Details
CVE-2026-47842	Applications using AesBytesEncryptor with the two-argument constructor or when passing a null IV generator and CBC as the encryption mode encrypt data with AES/CBC using a null (all-zero) initialization vector. Spring Security 7.1.0 Spring Security 7.0.0 - 7.0.6 Spring Security 6.5.0 - 6.5.11 Spring Security 6.4.0 - 6.4.18 Spring Security 5.8.0 - 5.8.27 Spring Security 5.7.0 - 5.7.25	6.5	More Details
CVE-2026-	A NoSQL/expression injection weakness exists in the LINQ-to-aggregation query translation layer of the MongoDB C# Driver, in both aggregation expression and query filter translation. When application-supplied values are embedded in certain query constructs, special elements contained within those values are not		More

81527	properly escaped before the resulting query is transmitted to the database, so portions of the value may be interpreted by the database as query logic rather than as data. A user able to supply values that an application incorporates into an affected query may thereby cause unintended data to be returned or query results to be altered.	6.5	Details
CVE-2026-81729	Dolibarr before 23.0.4 authorizes REST API document deletion against the wrong permission. Documents::delete() in htdocs/api/class/api_documents.class.php calls dol_check_secure_access_document() with the mode argument 'read' when handling DELETE /api/index.php/documents, while the sibling builddoc() path passes 'write', the correct mode for an operation that modifies stored data. An authenticated API user who holds only a read permission for a document-bearing module, for example societe:lire or facture:lire, and no create, write, delete or admin permission, therefore passes the check and can permanently delete that module's documents: third-party files, invoices, orders, proposals, project files and generated PDFs, with no recovery path. The call site is htdocs/api/class/api_documents.class.php:1276 in 23.0.3 and passes 'write' from 23.0.4 onward.	6.5	More Details
CVE-2026-77801	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 12.8 before 19.1.7, 19.2 before 19.2.5, and 19.3 before 19.3.1 that, under certain conditions, could have allowed an authenticated user to cause a denial of service affecting background job processing, due to missing object count limits.	6.5	More Details
CVE-2025-10903	GitLab has remediated an issue in GitLab EE affecting all versions from 11.10 before 19.1.7, 19.2 before 19.2.5, and 19.3 before 19.3.1 that, under certain conditions, an authenticated user could have caused denial of service, due to an unbounded loop triggered by specially crafted input in the SCIM user provisioning feature.	6.5	More Details
CVE-2026-59278	JsonKafkaHeaderMapper and DefaultKafkaHeaderMapper include java.net in their default trusted packages list. When these mappers are used — which is the default configuration for all @KafkaListener consumers — an external Kafka producer can inject a java.net.InetAddress type via the spring_json_header_types message header. Spring for Apache Kafka 4.1.0 Spring for Apache Kafka 4.0.0 - 4.0.6 Spring for Apache Kafka 3.0.0 - 3.3.16 Spring for Apache Kafka 2.9.0 - 2.9.14 Spring for Apache Kafka 2.8.12 and earlier	6.5	More Details
CVE-2026-55545	Yamcs is a mission control framework. Prior to 5.12.8 and 5.13.2, Yamcs WebSocket subscription handlers fail to enforce the privileges required by equivalent REST endpoints. PacketsApi.subscribePackets exposes the packets WebSocket topic without ObjectPrivilegeType.ReadPacket, ProcessingApi.subscribeAlgorithmStatus exposes the algorithm-status WebSocket topic without ObjectPrivilegeType.ReadAlgorithm, and MdbOverrideApi.subscribeMdbChanges exposes the mdb-changes WebSocket topic without SystemPrivilege.GetMissionDatabase. A low-privilege authenticated user can receive telemetry packets, algorithm status, and mission database change information outside the assigned authorization scope. This issue is fixed in versions 5.12.8 and 5.13.2.	6.5	More Details
CVE-2026-48548	Nagios Core before 4.5.12 contains a cross-site request forgery vulnerability in cmd.cgi where the CSRF protection mechanism passes validation when the NagFormId cookie is absent. Attackers can craft a malicious cross-site POST request to execute arbitrary Nagios commands as a currently authenticated user without their knowledge or consent.	6.5	More Details
CVE-2026-73209	An attacker that has valid credentials can send crafted compressed data that causes the affected process to exhaust its stack and crash. The affected process is terminated, which can cause degradation or denial of service for IMAP. Update to non-vulnerable version. No publicly available exploits are known.	6.5	More Details
CVE-2026-48549	Nagios Core before 4.5.13 and Nagios XI before 2026R1.5 contains a CSRF vulnerability in cmd.cgi. When no Cookie header is present, the double-submit cookie protection can be bypassed by supplying matching NagFormId and nagFormId values in the POST body, allowing a cross-site request to execute Nagios commands as a currently authenticated user.	6.5	More Details
CVE-2026-9548	An improper neutralization of input during web page generation ('Cross-site Scripting') vulnerability in extract domain in Synology Chat Server before 2.4.5-22148 allows remote authenticated users, via a UI interaction, to read or write restricted files and conduct limited denial-of-service attacks in DSM.	6.5	More Details
CVE-2026-81030	Mage AI does not confine the paths accepted by its browser-items API to the project directory. BrowserItemResource in mage_ai/api/resources/BrowserItemResource.py passes a caller-supplied path to the filesystem read and write helpers without calling the containment helper that the sibling FileContentResource and FileResource classes both use, so the resource contains no such call while those two contain several. A user holding the Viewer role, which grants read access within the project and nothing outside it, can therefore read any file the server process can read by supplying an absolute path. The permission model that would otherwise separate roles is not consulted for this route in the default configuration, because the setting that enables it defaults to false. Callers holding the Editor role additionally write through the same unconfined path, though that role is already able to execute code by design, so the boundary crossed by this flaw is the read available to the Viewer role.	6.5	More Details
CVE-2026-81280	Subscriber Sensitive Data Exposure in Print Barcode Labels for your WooCommerce products/orders <= 4.0.0 versions.	6.5	More Details
CVE-2026-18234	The MStore API WordPress plugin before 4.21.1 does not verify that the order targeted by its wallet payment handling belongs to the requester, and does not deduct the wallet balance for most payment methods, allowing any authenticated user, including Subscribers, to mark arbitrary orders as paid without any	6.5	More Details

	payment being taken.		
CVE-2026-82123	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Tangible Loops & Logic.	6.5	More Details
CVE-2026-81101	The configure command accepted any endpoint URL and stored it beside the user's access token. ConfigureCommand.execute in src/cli.ts persisted the value given to its endpoint option into the user profile without passing it through createSafeUrl in src/config.ts, the helper that already restricted the environment-variable form of the same setting to the vendor's own hosts over HTTPS. Because the connect path in src/mcp.ts attaches the stored token as a bearer credential on every request to the configured endpoint, a user who was persuaded to run configure with an endpoint of the attacker's choosing sent their personal access token to that destination on each subsequent invocation. Version 0.2.5 applies the same helper to the option.	6.5	More Details
CVE-2026-14697	net_ipv6_send_ns() in subsys/net/ip/ipv6_nbr.c allocates a transmit net_pkt for a Neighbor Solicitation. When it is called with a data packet pending on an unresolved neighbor and that neighbor's pending_queue is already non-empty (an NS is already outstanding), the function appends the data packet and returns early without ever sending the NS via net_send_data() or releasing it with net_pkt_unref(). The freshly allocated NS net_pkt and its attached TX buffers are held only by a local variable and are leaked permanently, never returning to CONFIG_NET_PKT_TX_COUNT / CONFIG_NET_BUF_TX_COUNT. The leaking branch sits on the normal IPv6 transmit path: net_ipv6_prepare_for_send() (called from net_if.c) invokes net_ipv6_send_ns() for any outbound or forwarded IPv6 packet whose next hop is not yet in the neighbor cache. An on-link (adjacent) attacker can drive it deterministically by sending a burst of request packets (for example ICMPv6 echo requests or UDP datagrams) that all spoof a single non-existent on-link source address: the node generates a reply to each, the first reply queues an NS, and every subsequent reply during the roughly three-second INCOMPLETE resolution window takes the leaking branch and loses one TX packet. Router-configured nodes forwarding attacker traffic toward a non-existent on-link host leak identically. Because the leaked packets are never reclaimed and CONFIG_NET_PKT_TX_COUNT defaults to only 4 (14 for Ethernet), a brief low-rate burst exhausts the TX pool. Once exhausted the node can no longer allocate any transmit packet and cannot send TCP/UDP, ARP/ND, or any reply at all, producing a complete and persistent network denial of service that does not self-heal until reboot. The fix releases the unsent NS packet with net_pkt_unref(pkt) before the early return.	6.5	More Details
CVE-2026-75460	XueZhiSi Open Source Exam System <= 3.9.0 has a privilege escalation vulnerability in the teacher-end interface POST /api/teacher/user/page/list. The role parameter in UserPageRequestVM is fully controllable by the requester.	6.5	More Details
CVE-2026-82547	A vulnerability was found in Linux Foundation Magma 1.9.0. The affected element is an unknown function of the file tasks/amf/amf_fsm.cpp of the component Registration Complete Message Handler. The manipulation results in improper authentication. The attack can be launched remotely. The exploit has been made public and could be used.	6.5	More Details
CVE-2026-40526	Volmarg Personal Management System contains a path traversal vulnerability that allows authenticated attackers to read arbitrary files by supplying absolute filesystem paths to the GET /public/get-file/{path} endpoint. The path route parameter is passed directly to file_get_contents() without canonicalization against a permitted base directory, enabling attackers to retrieve sensitive files accessible to the PHP-FPM worker process without using directory traversal sequences.	6.5	More Details
CVE-2026-40017	An attacker that can send mail to a user can craft a message header whose values are chosen to collide in an internal hash table, which makes the IMAP THREAD command consume CPU disproportionate to the size of the message. This is a separate issue from CVE-2026-40014 and is not addressed by that fix. Whenever a mail client issues a THREAD command on the affected mailbox, this can cause degradation or denial of service for IMAP. Monitor system for abnormal CPU usage, kill the offending process and remove the offending message from the affected mailbox. Update to non-vulnerable version. No publicly available exploits are known.	6.5	More Details
CVE-2026-82462	pac4j-oidc before 6.5.6 accepts OIDC callbacks carrying only an access token without authorization code or ID token validation. Attackers can substitute access tokens minted for other clients to create authenticated sessions without proper issuer, audience, nonce, or subject verification.	6.5	More Details
CVE-2026-77008	The HEL Online Classroom: AI-powered Online Classrooms WordPress plugin through 1.0.3 does not have any authorisation or authentication check when saving its settings, allowing unauthenticated users to overwrite them and repoint every online classroom, along with the shared secret those sessions are signed with, at infrastructure of their choosing.	6.5	More Details
CVE-2026-18233	The MStore API WordPress plugin before 4.21.1 does not verify that the order targeted by one of its delivery endpoints belongs to the requester, allowing any authenticated user, including Subscribers, to mark arbitrary orders as completed and paid without any payment being made.	6.5	More Details
CVE-2026-82634	Frappe Framework development builds contain an authorization flaw in the render_jinja_template endpoint that allows low-privileged users to render arbitrary Jinja templates by supplying raw template strings. Attackers with print permission on any document can execute arbitrary SELECT statements against unrelated tables, including reading password hashes from the __Auth table.	6.5	More Details

CVE-2026-52687	An attacker that has valid credentials can select a compression algorithm for the IMAP connection whose decompression state requires a large amount of memory, and open several such connections. The memory limit of the process is reached with only a few connections, terminating the process and all connections it handles, which can cause degradation or denial of service for IMAP. Disable IMAP compression. Alternatively limit the number of connections handled by a single imap-login process, though this has a performance impact. Update to non-vulnerable version. No publicly available exploits are known.	6.5	More Details
CVE-2026-14696	When Ethernet bridging is enabled (CONFIG_NET_ETHERNET_BRIDGE), eth_bridge_input_process() in subsys/net/l2/ethernet/bridge/bridge_input.c decides how each frame received on a bridge member interface is handled. For frames that must also be delivered to the local stack, the code called eth_bridge_handle_locally() and returned NET_OK. That helper does not consume the packet — it only calls bridge_iface_recv() (via virtual_recv()), which returns NET_CONTINUE without taking ownership of pkt. The NET_OK verdict then propagates through ethernet_recv() up to processing_data() in subsys/net/ip/net_core.c, where NET_OK is interpreted as "the packet was consumed, do not free it." Because no consumer actually took ownership, the RX net_pkt is never returned to the pool and is leaked. The concretely reproducible leak occurs for frames whose EtherType has no registered L3 handler when CONFIG_NET_ETHERNET_FORWARD_UNRECOGNISED_ETHERTYPE is set (default y when CONFIG_NET_SOCKETS_PACKET is enabled): the fall-through L3 dispatch does not overwrite the NET_OK verdict, so ethernet_recv() returns NET_OK and the buffer is never released. Any device on a bridged L2 segment can emit broadcast/multicast frames carrying an arbitrary EtherType with no authentication. Each such frame permanently consumes one buffer from the finite RX pool (CONFIG_NET_PKT_RX_COUNT), so a brief broadcast flood exhausts the pool and the device can no longer receive traffic until it is rebooted — a persistent denial of service. There is no confidentiality or integrity impact. The fix makes eth_bridge_handle_locally() propagate the real net_verdict and return NET_CONTINUE for locally-kept frames, writing the bridge interface back through a new dst_iface out-parameter so the packet follows the normal receive path and is unreferenced exactly once.	6.5	More Details
CVE-2026-82250	gitoxide gix-packetline versions before 0.21.5 contain a panic vulnerability in the TextRef implementation that occurs when processing side-band packet lines with empty payloads. A malicious Git server can send a crafted side-band packet to trigger an index out of bounds panic, aborting the client process during fetch operations without authentication.	6.5	More Details
CVE-2026-40014	An attacker that can send mail to a user can craft a message header that makes the IMAP THREAD command consume CPU disproportionate to the size of the message. When a mail client issues a THREAD command on the affected mailbox, this can cause degradation or denial of service for IMAP. Monitor system for abnormal CPU usage, kill the offending process and remove the offending message from the affected mailbox. Update to non-vulnerable version. No publicly available exploits are known.	6.5	More Details
CVE-2026-81762	Subscriber Broken Access Control in Booking and Rental Manager <= 2.7.6 versions.	6.5	More Details
CVE-2026-77010	The HEL Online Classroom: AI-powered Online Classrooms WordPress plugin through 1.0.3 does not perform authorisation checks on its REST API routes and does not consistently enforce the per-class access code, allowing unauthenticated users to obtain a signed meeting join link for any classroom, including one protected by an access code, and to join it with moderator privileges.	6.5	More Details
CVE-2026-82643	WWBN AVideo contains an unauthenticated credential submission vulnerability in plugin/Live/api/preauthorize.json.php that accepts credentials over GET without rate limiting. Attackers can submit correct credentials repeatedly to trigger uncapped two-factor confirmation emails and perform sustained password guessing attacks against user accounts.	6.5	More Details
CVE-2026-80210	FrontAccounting through 2.4.20 generates a CSRF token in end_form() in includes/ui/ui_controls.inc and embeds it as the _token hidden field in every form it renders, but only admin/users.php and admin/change_current_user_password.php call check_csrf_token() to validate it. No financial transaction handler validates the token, including gl/gl_journal.php, gl/gl_bank.php, purchasing/supplier_invoice.php, sales/customer_invoice.php, sales/customer_payments.php and admin/company_preferences.php, so those endpoints act on POST data with no origin check. An attacker who gets an authenticated user to load a page under attacker control can auto-submit a cross-origin form to any of them and have the forged journal entry, invoice, customer payment, bank transaction or company configuration change recorded under the victim's session.	6.5	More Details
CVE-2026-81034	Netmaker disables certificate verification on the connection to the configured mail server. The sender in pro/email/smtp.go assigns a TLS configuration whose skip-verify field is set to true unconditionally, directly beneath a comment stating that the setting should be false in production. No configuration value governs it and no code path restores verification, so the client accepts any certificate the mail server presents, including one an interposing party supplies. Mail that Netmaker sends over that connection includes password-reset messages carrying single-use tokens and user invitations carrying enrolment links, so a party positioned on the path between the server and its mail relay can read those messages in transit and use a captured reset token before the intended recipient does. The setting is absent from the development branch but present in the latest release.	6.5	More Details
	MariaDB Connector/Node.js is used to connect applications developed on Node.js to MariaDB and MySQL databases. Prior to 3.2.4, 3.3.3, 3.4.6, and 3.5.3, MariaDB Connector/Node.js permits SQL injection when attacker-controlled Buffer parameters are escaped client-side under the big5, gbk, sjis, cp932, or gb18030		

CVE-2026-55855	client character sets. PacketOutputStream.writeBufferEscape in lib/io/packet-output-stream.js escaped bytes without the charset-aware getMbRecognizer logic in lib/misc/charset-mb.js. The server SQL lexer runs my_ismbchar before escape processing, so an attacker-controlled lead byte can consume the inserted 0x5C backslash as a multibyte trail byte and leave the following 0x27 quote unescaped, terminating the string literal and allowing arbitrary SQL. The default utf8mb4 character set and parameters sent through the execute binary prepared-statement path are not affected. Successful exploitation can expose or modify data available to the database account. This issue is fixed in versions 3.2.4, 3.3.3, 3.4.6, and 3.5.3.	6.5	More Details
CVE-2026-59274	The UnZipTransformer does not limit decompressed entry size or entry count when processing archives. Consequently, an attacker can send a zip archive that can exhaust JVM heap memory, causing a denial-of-service outage. Spring Integration 7.1.0 Spring Integration 7.0.0 - 7.0.5 Spring Integration 6.5.0 - 6.5.10 Spring Integration 6.4.0 - 6.4.12	6.5	More Details
CVE-2026-80189	LeafWiki extracts an uploaded ZIP archive without limiting how much data it will write. ZipExtractor.ExtractToDir in internal/importer/zip_extractor.go opens each entry and copies it to the destination with io.Copy, which runs to the end of the decompressed stream, so only the size of the uploaded archive is bounded and the size it expands to is not. The import route that reaches this code requires the Editor or Admin role, and the upload itself is capped at 500 MiB compressed. Because a ZIP entry can compress at a very high ratio, an archive well inside that cap can expand to hundreds of gigabytes as it is written out. The extraction directory defaults to a location under the operating system temporary directory, so the written data consumes the disk backing that path, which on a tmpfs-backed temporary directory is memory. A user holding the Editor role can therefore exhaust the storage the service depends on and keep it from serving, using far more resource than the upload limit alone would permit.	6.5	More Details
CVE-2026-5510	The GiveWP – Donation Plugin and Fundraising Platform plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'give_form' shortcode in all versions up to, and including, 4.14.4. This is due to insufficient input sanitization and output escaping on the continue_button_title and display_style shortcode attributes, which are passed through sanitize_text_field() but not properly escaped when output in HTML data attributes. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-15798	The Smart Slider 3 plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'slider' Block Attribute in all versions up to, and including, 3.5.1.38 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The injected scripts execute specifically when a user opens the affected post in the WordPress block editor, making Editors and Administrators the primary targets.	6.4	More Details
CVE-2026-6178	The Betheme theme for WordPress is vulnerable to Stored Cross-Site Scripting via the theme's 'icon_box_2' shortcode in all versions up to, and including, 28.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-47864	SerializingHttpMessageConverter deserializes the body of incoming HTTP requests with a raw java.io.ObjectInputStream and no class filtering. Any request with Content-Type application/x-java-serialized-object whose body resolves to a Serializable type is read directly via readObject(). If an application using this converter on an inbound HTTP endpoint has any known Java deserialization "gadget" on its classpath, a remote, unauthenticated attacker can achieve arbitrary code execution. Spring Integration 7.1.0 Spring Integration 7.0.0 - 7.0.5 Spring Integration 6.5.0 - 6.5.10 Spring Integration 6.4.0 - 6.4.12 Spring Integration 5.5.21 and earlier	6.4	More Details
CVE-2026-2388	The Reviews and Rating – Google Reviews plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 5.10. This is due to the wp_display() shortcode handler, used by multiple shortcodes, allowing attacker-controlled html_tags values to define raw HTML tags and then embedding untrusted vicinity content inside those tags. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-5092	The Greenshift – animation and page builder blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the customapi action handler in versions up to, and including, 12.8.9. This is due to insufficient sanitization of API responses before output via innerHTML. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the injected page.	6.4	More Details
CVE-2026-16654	The Avada (Fusion) Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'size' Shortcode Attribute in all versions up to, and including, 3.15.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. WordPress's wp_kses_post filter does not neutralize the payload because the injected content resides entirely within a shortcode attribute string containing no HTML angle brackets, causing kses to pass it through unchanged at save time.	6.4	More Details
	The All-in-One WP Migration Unlimited Extension plugin for WordPress is vulnerable to Stored Cross-Site		

CVE-2026-6128	Scripting via the 'ai1wm_backups_path' parameter in all versions up to, and including, 2.84. This is due to insufficient input sanitization and output escaping on user-supplied attributes combined with missing authorization checks on the settings() function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever an administrator accesses the plugin settings page. The vulnerability was partially patched in version 2.84.	6.4	More Details
CVE-2026-82081	wallabag 2 through 2.6.14 allows SSRF because a crafted title or content field is mishandled during PDF export.	6.4	More Details
CVE-2026-54746	Hatchet is a platform for orchestrating background tasks, AI agents, and durable workflows at scale. From 0.40.0 until 0.91.1, the Dispatcher gRPC service does not verify that a request's worker ID belongs to the tenant identified by the bearer-token context in Dispatcher/UpsertWorkerLabels and Dispatcher/Unsubscribe. An authenticated owner of any tenant who guesses another tenant's worker UUID can overwrite that worker's affinity labels or disconnect the worker from the dispatcher. This can cause cross-tenant integrity impact and denial of service on multi-tenant Hatchet Cloud or shared self-hosted deployments. Single-tenant deployments are not practically affected because the attacker and target tenant are the same. This issue is fixed in version 0.91.1.	6.4	More Details
CVE-2026-14366	The Silicon Labs SiWx917 WiFi driver's transmit callback siwx91x_send() in drivers/wifi/siwx91x/siwx91x_wifi.c frees a network packet it does not own. In the Zephyr TX path the net_pkt is owned by the L2/networking stack; the driver only borrows it to copy the frame bytes into a local net_buf. Before the fix, after transmitting, siwx91x_send() additionally called net_pkt_unref(pkt) on the caller-owned packet, dropping its last reference and returning it to the shared packet pool prematurely. This code path is compiled in by default (CONFIG_WIFI_SILABS_SIWX91X_NET_STACK_NATIVE). The caller, ethernet_send() in subsys/net/l2/ethernet/ethernet.c, keeps using the packet after the driver returns: it reads net_pkt_get_len(pkt), updates TX statistics, and then performs its own net_pkt_unref(pkt). Because the driver already released the packet, these are use-after-free reads followed by a second unref (a double free). When concurrent network activity recycles the freed slab slot between the two unrefs, the trailing unref decrements a different, live packet's reference count and frees it, corrupting the net_pkt pool shared by both the receive and transmit paths. The defect is exercised by ordinary transmission over the native-stack SiWx917 WiFi interface, and an adjacent attacker on the same WiFi network can induce transmissions (for example ARP or ICMP echo replies, or TCP handshakes) to drive the path. The primary observable impact is loss of availability (transmit hangs and crashes from pool corruption), with race-dependent memory corruption of the kernel networking buffer pool. The fix removes the erroneous net_pkt_unref(pkt) from siwx91x_send(); the driver's receive-path unref, which correctly frees a packet the driver itself allocated, is unaffected.	6.4	More Details
CVE-2026-19294	IBM Langflow OSS 1.0.0 through 1.11.1 could allow a remote authenticated attacker to execute and read any user's private flow due to improper authorization.	6.4	More Details
CVE-2026-3002	The Gutenverse – Ultimate WordPress FSE Blocks Addons & Ecosystem plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the multiple blocks in all versions up to, and including, 4.0.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-3129	The LiteSpeed Cache plugin for WordPress is vulnerable to Stored Cross-Site Scripting via crafted `<img>` tag attributes in all versions up to, and including, 7.7. This is due to a flawed regular expression that is used to strip `width` and `height` attributes from images when the "Lazy Load Images" and "Add Missing Sizes" features are enabled. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-62342	HCL IntelliOps Event Management (IEM) is affected by a Session Deletion Vulnerability. It may allow improper handling of user sessions, resulting in sessions not being fully terminated after logout or deletion.	6.4	More Details
CVE-2026-3423	The Envira Gallery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the gallery 'description' configuration field in all versions up to, and including, 1.12.4 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 a page displaying the gallery with a description enabled.	6.4	More Details
CVE-2026-82833	A vulnerability was identified in Doccano Open Source Annotation Tools for Machine Learning Practitioners and Auto Labeling Pipeline Module to Annotate a Document Automatically up to 1.8.5. Affected by this issue is the function ExampleDetail of the file /v1/projects/1/examples/ of the component Project Example Detail Endpoint. Such manipulation leads to improper access controls. The attack may be launched remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-82540	A vulnerability was identified in itsourcecode Sales and Inventory System 1.0. Affected is an unknown function of the file /pages/cust_searchfrm.php. The manipulation of the argument ID leads to sql injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.	6.3	More Details
CVE-2026-	A vulnerability was determined in dibo-software diboot 3.8.0. This affects an unknown part of the file /api/iam/tenant/resource of the component Tenant Resource Assignment Handler. Executing a manipulation		More

82818	of the argument tenantId can lead to improper access controls. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	Details
CVE-2026-47856	Spring Integration's JSON to object conversion uses the json__TypeId__ header to choose the deserialization target type, and resolves that header value to a class with ClassUtils.forName and no type/package allow-list. Spring Integration 7.1.0 Spring Integration 7.0.0 - 7.0.5 Spring Integration 6.5.0 - 6.5.10 Spring Integration 6.4.0 - 6.4.12 Spring Integration 5.5.21 and earlier	6.3	More Details
CVE-2026-82679	A security flaw has been discovered in diem-project diem up to 5.1.3. The impacted element is an unknown function of the file dmFrontPlugin/lib/dmWidget/media/dmWidgetContentBaseMediaForm.php of the component Widget Editor. Performing a manipulation results in unrestricted upload. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-59322	The EmbeddedHeadersJsonMessageMapper defaults to an overly permissive header parsing posture in its constructor. When decodeNativeFormat processes raw byte payloads, it deserializes embedded JSON headers into a plain Map and constructs a GenericMessage with MutableMessageHeaders without sanitizing or filtering untrusted header names by default. Spring Integration 7.1.0 Spring Integration 7.0.0 - 7.0.5 Spring Integration 6.5.0 - 6.5.10 Spring Integration 6.4.0 - 6.4.12 Spring Integration 5.5.21 and earlier	6.3	More Details
CVE-2026-9668	With legitimate user credentials in hand, attackers can construct malicious SQL statements to bypass authentication logic and execute arbitrary database queries directly. This will consequently lead to slow database queries and expanded query coverage. This vulnerability features a low exploitation threshold, wide scope of impact, requires no external privilege escalation, and is classified as a high-priority fix.	6.3	More Details
CVE-2026-76798	The MongoSQL Transition Readiness Tool writes query text and user names read from BI Connector log files into its generated HTML report without encoding them for that output context. A user able to issue queries through the BI Connector can influence log content so that markup supplied in a query is interpreted by the browser when an operator later generates and opens the report, which may disclose other users' logged query text and user names to an external party or present misleading content to the operator. Generating a report over logs containing the affected entries and opening that report in a browser is required.	6.3	More Details
CVE-2026-76797	The MongoSQL Transition Readiness Tool writes database and collection names into its generated CSV reports without neutralizing leading characters that spreadsheet applications treat as formulas. A user with write privileges on the cluster can choose a namespace name that is later evaluated as a formula when an operator opens the generated report in a spreadsheet application, which may result in unintended disclosure of report contents or execution of external content on the operator's workstation. Generating a report for the affected namespace and opening it in a spreadsheet application is required.	6.3	More Details
CVE-2026-47861	An unauthenticated remote attacker who can send a single UDP packet to a Spring Integration UDP inbound adapter can cause the server to emit an outbound UDP datagram to an arbitrary internal or external host and port of the attacker's choosing. Spring Integration 7.1.0 Spring Integration 7.0.0 - 7.0.5 Spring Integration 6.5.0 - 6.5.10 Spring Integration 6.4.0 - 6.4.12 Spring Integration 5.5.21 and earlier	6.3	More Details
CVE-2026-82878	DataEase versions before 2.10.26 omit object-level authorization checks on geographic information, dashboard linkage, and chart detail REST endpoints, allowing authenticated users to access resources belonging to other users. Attackers can overwrite or delete map geometry, modify dashboard linkages, and retrieve chart metadata and configuration for resources they do not own by supplying arbitrary identifiers in requests.	6.3	More Details
CVE-2026-82421	A vulnerability was identified in itsourcecode Sales and Inventory System 1.0. This issue affects some unknown processing of the file /pages/emp_edit.php. The manipulation of the argument ID leads to sql injection. The attack may be initiated remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2026-82479	A vulnerability was identified in NASA cFS up to 7.0.1. Impacted is the function OS_read of the file modules/protocol/tcp/fsw/src/sbn_tcp_if.c of the component SBN TCP Module. Such manipulation of the argument MsgSz leads to buffer overflow. The attack must be carried out from within the local network. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-82879	DataEase before 2.10.26 contains multiple access control defects in the sharing link module. Tickets are not bound to the target share UUID, so a valid ticket issued for one share can be reused against another (ShareTicketManage.validateTicket / POST /de2api/share/proxyInfo). The POST /de2api/share/validate endpoint issues a LinkToken after password verification without requiring a ticket, bypassing the 'ticket mandatory' policy. Additionally, the ticket create and delete endpoints (POST /de2api/ticket/saveTicket, POST /de2api/ticket/delTicket) lack share-ownership checks, allowing an authenticated user who knows another user's ticket to modify, rebind, or delete it (denial of service), and GET /de2api/share/queryRelationByUserId/{uid} allows authenticated users to enumerate other users' share mappings.	6.3	More Details
CVE-2026-82553	A vulnerability was detected in sambitraj Student Management System up to 56ba287f2e9031523ccb4244cb6e3fe530e4e5d5. Affected by this issue is the function mysqli_query of the file student_dashboard.php of the component Student Dashboard. The manipulation of the argument roll_no results in improper authorization. The attack may be performed from remote. The exploit is now public and may be used. This product utilizes a rolling release system for continuous delivery, and as such, version	6.3	More Details

	information for affected or updated releases is not disclosed. The project was informed of the problem early through an issue report but has not responded yet.		
CVE-2026-82484	A flaw has been found in itsourcecode Sales and Inventory System 1.0. Affected is an unknown function of the file /pages/emp_searchfrm.php. This manipulation of the argument ID causes sql injection. The attack may be initiated remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2026-81758	Subscriber Broken Access Control in OwnerRez API <= 1.2.6 versions.	6.3	More Details
CVE-2026-82545	A vulnerability has been found in itsourcecode Sales and Inventory System 1.0. Impacted is an unknown function of the file /pages/sup_searchfrm.php. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2026-82620	A security flaw has been discovered in Soarkey StudentManagement and 学生信息管理系统 up to e08f7f1d5015af407aa4cca0ada3dea189b4937e. This affects the function CourseDao.course_ranking of the file code/src/dao/CourseDao.java. Performing a manipulation of the argument cno results in sql injection. It is possible to initiate the attack remotely. The exploit has been released to the public and may be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-19197	A user with organization administrator permissions can delete dashboard snapshots belonging to other organizations on the same Grafana instance, and can recover a snapshot's secret delete key using only its public share key (broken access control).	6.3	More Details
CVE-2026-82696	A weakness has been identified in itsourcecode Sales and Inventory System 1.0. The affected element is an unknown function of the file /pages/inv_searchfrm.php. This manipulation of the argument ID causes sql injection. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks.	6.3	More Details
CVE-2026-82556	A vulnerability was found in Forgejo up to 15.0.4. This issue affects the function net.LookupIP of the file services/migrations/allowlist/is_migrate_allowed.go of the component Repository Migration Handler. Performing a manipulation results in server-side request forgery. The attack can be initiated remotely. The exploit has been made public and could be used. The patch is named b313bb83f5ff22bcc0378e0e0ca7bbd58303f168. It is recommended to apply a patch to fix this issue. The project maintainer explains: "I don't intend to backport this to v15 or v16 as it is a breaking change."	6.3	More Details
CVE-2026-82487	A vulnerability was determined in Beetel 450TC3 01.00.00_01. This affects an unknown part. Executing a manipulation can lead to weak password recovery. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-82609	A vulnerability was identified in itsourcecode Sales and Inventory System 1.0. This impacts an unknown function of the file /pages/inv_edit.php. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.	6.3	More Details
CVE-2026-82424	A weakness has been identified in PHPGurukul Student Information System 1.0. Affected by this vulnerability is an unknown functionality of the file /student_edit1.php. Executing a manipulation of the argument ID can lead to sql injection. The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks.	6.3	More Details
CVE-2026-82817	A vulnerability was found in dibo-software diboot 3.8.0. Affected by this issue is some unknown functionality of the file /admin/ of the component Tenant Administrator Management API. Performing a manipulation of the argument tenantId results in improper access controls. The attack may be initiated remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-82816	A vulnerability has been found in dibo-software diboot 3.8.0. Affected by this vulnerability is an unknown functionality of the file /api/ai-session/ of the component AI Session Endpoint. Such manipulation leads to authorization bypass. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-82541	A security flaw has been discovered in itsourcecode Sales and Inventory System 1.0. Affected by this vulnerability is an unknown functionality of the file /pages/sup_edit.php. The manipulation of the argument ID results in sql injection. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks.	6.3	More Details
CVE-2026-82422	A security flaw has been discovered in itsourcecode Sales and Inventory System 1.0. Impacted is an unknown function of the file /pages/emp_del.php. The manipulation of the argument ID results in sql injection. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks.	6.3	More Details
CVE-2026-82905	A vulnerability was detected in sdcb chats up to 1.12.0. This affects the function McpController of the file src/BE/web/Controllers/Users/Mcps/McpController.cs of the component fetch-tools Endpoint. The manipulation results in server-side request forgery. The attack may be launched remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in	6.3	More Details

	any way.		
CVE-2026-82485	A vulnerability has been found in itsourcecode Sales and Inventory System 1.0. Affected by this vulnerability is an unknown functionality of the file /pages/pro_edit.php. Such manipulation of the argument ID leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2026-81834	A weakness has been identified in RooCodeInc Roo-Code up to 3.51.1. Affected by this issue is the function ExecaTerminalProcess of the component README File Handler. Executing a manipulation can lead to code injection. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks. Multiple isses were reported to the vendor beforehand. They explain, that "they all apply to Roo Code, a project we no longer support - the repository was archived a while ago, and we don't encourage anyone to use it." This vulnerability only affects products that are no longer supported by the maintainer.	6.3	More Details
CVE-2026-81845	A vulnerability has been found in arben-adm mcp-sequential-thinking up to 0.5.0. Impacted is the function import_session/export_session of the file mcp_sequential_thinking/server.py of the component Import Session/Export Session. Such manipulation of the argument file_path leads to path traversal. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 0.6.0 is recommended to address this issue. The name of the patch is 2fad3ee8ab1d0868b6c1afb5895bc336a10e5267. Upgrading the affected component is recommended.	6.3	More Details
CVE-2026-81837	A flaw has been found in RooCodeInc Roo-Code up to 3.51.1. This issue affects the function path.resolve of the file src/core/tools/ApplyPatchTool.ts of the component ApplyPatchTool. This manipulation causes path traversal. It is possible to initiate the attack remotely. The exploit has been published and may be used. Multiple isses were reported to the vendor beforehand. They explain, that "they all apply to Roo Code, a project we no longer support - the repository was archived a while ago, and we don't encourage anyone to use it." This vulnerability only affects products that are no longer supported by the maintainer.	6.3	More Details
CVE-2026-81686	openssl_encrypt 1.4.x before 1.4.9 contains an optional D-Bus crypto service whose org.freedesktop.DBus.Properties.Set method performs neither a polkit authorization check nor value validation. Any local user on the system bus can call Set without authorization and set MaxConcurrentOperations (to 0/negative, causing the concurrency gate to refuse all subsequent operations, or to a huge value removing the limit) or the unbounded DefaultTimeout, resulting in a persistent denial of service of the root daemon. The D-Bus service exists only on the 1.4.x line and was removed in 1.5.x.	6.2	More Details
CVE-2026-3686	IBM Cloud Pak for Data System 11.3.0.2 through Interim Fix 001 is vulnerable to a denial of service due to improper limitation of resources.	6.2	More Details
CVE-2026-81720	openssl_encrypt before 1.4.9 fails to validate the memory_cost parameter from identity file protection blocks, allowing attackers to trigger out-of-memory conditions during key derivation. Attackers with write access to local identity stores can craft malicious identity files with excessive memory_cost values that cause the host to crash when unlocking identities before authentication.	6.2	More Details
CVE-2026-81682	openssl_encrypt versions before 1.4.9 contain an insecure file permissions vulnerability in the desktop GUI that writes decrypted plaintext with world-readable default permissions. Attackers can read decrypted output files created by the GUI as unprivileged local users on multi-user systems.	6.2	More Details
CVE-2026-81684	In openssl_encrypt (pip package openssl-encrypt) versions <= 1.4.8, the desktop GUI passes the steganography password to the CLI child process on the command line via the --stego-password argument (on both encrypt and decrypt paths) instead of via an environment variable as done for the main password. Any local user can read the steganography password from /proc/<pid>/cmdline for the lifetime of the subprocess. Fixed in 1.4.9.	6.2	More Details
CVE-2026-19854	When the ClickHouse plugin uses Native protocol (the default) with PDC or secure SOCKS, it asks for TLS but the connection library ignores that and talks to ClickHouse in the clear. Username, password, queries, and results can be read on the hop after the proxy. The server certificate is never checked, and a configured client certificate is not sent.	6.1	More Details
CVE-2026-39275	Cross Site Scripting vulnerability in Cockpit CMS v.2.13.5 and before allows a remote attacker to execute arbitrary code via the item.php, field-select.js and tags.js components	6.1	More Details
CVE-2026-82324	A flaw was found in the file-iff (IFF/ILBM) plugin in GIMP. When processing a specially crafted IFF/ILBM image file, the plugin does not properly validate the HAM row size and improperly handles cases where the number of color planes (nPlanes) is zero. This causes a row size mismatch that bypasses memory bounds checking, resulting in heap out-of-bounds reads. This issue can result in an application crash, leading to a denial of service or a limited information disclosure of heap memory contents.	6.1	More Details
CVE-2025-63607	TechStore 1.0 is vulnerable to Cross Site Scripting (XSS). In contact_display, the application echoes the id parameter verbatim into the rendered page, permitting execution of attacker-supplied JavaScript in users browser.	6.1	More Details
CVE-2026-	A flaw was found in the file-ico plugin in GIMP. When processing a specially crafted ICO image file, the plugin does not properly validate the used_clrs (palette count) parameter. This incorrect validation leads to	6.1	More

82328	improper memory bounds checking, resulting in a heap out-of-bounds read. This issue can result in an application crash, leading to a denial of service or a limited information disclosure of heap memory contents.		Details
CVE-2026-4246	The ElementsKit Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 's' parameter of the Advanced Search REST endpoint in all versions up to, and including, 4.10.1 due to insufficient input sanitization and output escaping. The REST endpoint at /wp-json/elementskit/v1/advanced-search uses permission_callback set to __return_true, allowing unauthenticated access. Search terms are stored in the ekit_advanced_search_popular_keyword WordPress option via update_option(). While sanitize_text_field() is applied, it does not encode double quotes, and the stored keywords are rendered in HTML attributes via sprintf without esc_attr(), allowing attribute injection. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user triggers the "no results" popular keywords view on pages using the Advanced Search widget.	6.1	More Details
CVE-2026-82330	A flaw was found in the file-pvr plugin in GIMP. When processing a specially crafted PVR image file, the VQ (compressed) decoder does not properly perform memory bounds checking. This missing validation results in a heap out-of-bounds read. This issue can result in an application crash, leading to a denial of service or a limited information disclosure of heap memory contents.	6.1	More Details
CVE-2026-50980	Cross-Site Scripting (XSS) vulnerability in the DNS lookup/management component of oPanel before v1.20.25 allows remote attackers to execute arbitrary JavaScript and perform session hijacking via a crafted DNS TXT record	6.1	More Details
CVE-2026-76986	Improper neutralization of input during web page generation in Apache Wicket. org.apache.wicket.markup.html.form.AbstractSingleSelectChoice, the base class of DropDownChoice, writes the body of the default option — the entry shown when no choice is selected — into the markup as it is, while every other option body in the same select is escaped according to the escape-model-strings setting. The body comes from getNullValidDisplayValue() or getNullKeyDisplayValue(), both of which are protected, so what they return is not necessarily the plain text the default implementation reads from a resource bundle. An application is affected where it overrides one of those methods and returns a value holding data an attacker can influence, or where its own nullValid or null bundle entry holds such a value. The bundles shipped with Wicket contain plain text. RadioChoice overrides getDefaultChoice to emit no default option and is not affected. As a workaround, escape the value in the override. This issue affects Apache Wicket: from 8.0.0 through 8.18.0, from 9.0.0 through 9.23.0, from 10.0.0 through 10.10.0. Older, unsupported releases from 1.5.0 onwards are also affected. Users are recommended to upgrade to version 8.19.0, 9.24.0 or 10.11.0, which fix the issue.	6.1	More Details
CVE-2026-37710	Cross Site Scripting vulnerability in Omeka S v.4.2.0 allows a remote attacker to execute arbitrary code via the site navigation custom URL function	6.1	More Details
CVE-2026-5953	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Ceviz Informatics Inc. Web Design allows Reflected XSS. This issue affects Web Design: through 25082026.	6.1	More Details
CVE-2026-59281	Spring MVC and WebFlux applications that obtain a data-binding Errors instance with HTML escaping enabled and then render field errors using the no-argument Errors.getFieldErrors() or Errors.getFieldError() accessors are vulnerable to arbitrary HTML/JavaScript code injection, potentially resulting in a reflected cross-site scripting (XSS) vulnerability. Spring Framework 7.0.0 - 7.0.8 Spring Framework 6.2.0 - 6.2.19 Spring Framework 6.1.0 - 6.1.28 Spring Framework 6.0.0 - 6.0.30 Spring Framework 5.3.0 - 5.3.49 Spring Framework 5.2.25.RELEASE and earlier	6.1	More Details
CVE-2026-5800	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Dayneks Software Industry and Trade Inc. E-Commerce Platform allows Reflected XSS. This issue affects E-Commerce Platform: through 28082026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.1	More Details
CVE-2026-81334	darknet subscripts its layer array with an index taken from a configuration file without checking it against the array's length. The array is allocated in src-lib/darknet_network.cpp as xcalloc(net.n, sizeof(Darknet::Layer)), sized to exactly the number of layer sections the file declares. The shortcut, scale_channels and sam sections supply that index through their from field and the route section through its layers field, and parse_shortcut_section in src-lib/darknet_cfg.cpp reads net.layers[index].outputs with no bounds check, which reads past the allocation. The dispatch loop in create_network then reuses the same index to assign net.layers[l.index].use_bin_output and net.layers[l.index].keep_delta_gpu, writing past the allocation at an offset the file controls, with a fixed one-byte value. Parsing a crafted configuration file is sufficient: the parse runs before any weights file is opened and needs no non-default option, so the result is a reliable crash and a write whose location, though not its value, is chosen by whoever supplied the file.	6.1	More Details
CVE-2026-82343	A flaw was found in the file-psd plugin in GIMP. When processing a specially crafted PSD image file, the plugin does not properly validate the channel-count parameter. This incorrect validation leads to improper memory bounds checking, resulting in both a heap out-of-bounds read and a stack out-of-bounds access. This issue can result in an application crash, leading to a denial of service or a limited information disclosure of memory contents.	6.1	More Details
CVE-2026-47883	UrlHandlerFilter can be vulnerable to an open redirect when configured with very broadly matching patterns. The issue applies to the filter variants in both Spring MVC and Spring WebFlux. Spring Framework 7.0.0 -	6.1	More Details

	7.0.8 Spring Framework 6.2.0 - 6.2.19		
CVE-2026-82451	Formwork through 2.3.14 contains a stored cross-site scripting vulnerability in visit tracking that records the Referer header host unescaped. Unauthenticated attackers can craft malicious Referer headers to inject markup that executes in administrator browsers when viewing the Statistics panel.	6.1	More Details
CVE-2026-82018	IGEL OS 12 before 12.9.0, 12.8.3 LTS and IGEL OS 11 before 11.11.150 contain a secure boot bypass vulnerability in the GRUB boot stage that allows physically present attackers to gain unauthorized root access by placing an unsigned empty file named igel.conf on a partition. Attackers can exploit GRUB's fail-open signature verification behavior to drop into an interactive GRUB prompt, then boot the device's own kernel with additional command-line arguments to obtain a root shell with the disk unlocked while leaving TPM PCR values unaltered.	6.1	More Details
CVE-2026-47848	In specific scenarios involving WebSocket handshake redirects to a different origin, the Reactor Netty WebSocket client may leak credentials. In order for this to happen, the HTTP client must have been explicitly configured to follow redirects. Reactor Netty 1.3.0 - 1.3.6 Reactor Netty 1.1.0 - 1.2.18 Reactor Netty 1.0.52 and earlier	6.1	More Details
CVE-2026-82464	pac4j-core before 6.5.6 contains an open redirect vulnerability in DefaultLogoutLogic.perform() that accepts backslash-prefixed logout redirect targets matching logoutUrlPattern. Attackers can craft logout links with backslash-prefixed external hosts that browsers normalize into network-path references, redirecting victims to attacker-controlled sites after logout.	6.1	More Details
CVE-2026-47887	A Spring MVC application that uses UrlFileNameViewController that is mapped with an end-of-path, and does not have a configured prefix is vulnerable to an open redirect. Spring Framework 7.0.0 - 7.0.8 Spring Framework 6.2.0 - 6.2.19 Spring Framework 6.1.0 - 6.1.28 Spring Framework 6.0.0 - 6.0.30 Spring Framework 5.3.0 - 5.3.49 Spring Framework 5.2.25.RELEASE and earlier	6.1	More Details
CVE-2026-5738	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in BilPark Informatics Technologies Industry and Trade Inc. DoXBASE allows Cross Zone Scripting. This issue affects DoXBASE: through 27082026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.1	More Details
CVE-2026-11747	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Seres Software syWEB allows Reflected XSS. This issue affects syWEB: through 27082026. NOTE: The vendor was contacted and it was learned that the product is not supported.	6.1	More Details
CVE-2026-82646	WWBN AVideo contains an unauthenticated reflected cross-site scripting vulnerability in the url2Embed.json.php endpoint that allows attackers to inject malicious scripts by supplying URLs with HTML metacharacters. Attackers can mint an encrypted evideo payload containing unescaped markup, then deliver it as a legitimate-looking link on the site's own domain to execute JavaScript in victims' sessions and steal cookies or CSRF tokens.	6.1	More Details
CVE-2026-82868	@pdfme/schemas before 5.5.9 contains a cross-site scripting vulnerability in the SVG schema plugin that renders user-supplied SVG content directly to innerHTML without sanitization. Attackers can inject malicious SVG with embedded scripts, event handlers, or foreignObject elements to execute arbitrary JavaScript in users' browsers when viewing or filling templates.	6.1	More Details
CVE-2026-82867	@pdfme/schemas before 5.5.9 contains a cross-site scripting vulnerability in the Select schema plugin that fails to sanitize option values before interpolating them into HTML via innerHTML. Attackers can supply malicious templates with crafted option values containing HTML and JavaScript to execute arbitrary code in users' browsers.	6.1	More Details
CVE-2026-82647	WWBN AVideo contains a cross-site request forgery vulnerability in sendEmail.json.php that allows authenticated administrators to send mail from the site's contact address by bypassing origin checks and captcha validation. Attackers can craft a malicious web page that, when visited by an authenticated admin, sends emails with attacker-controlled subject and body to arbitrary recipients, passing SPF/DKIM/DMARC validation for phishing and brand impersonation attacks.	6.1	More Details
CVE-2026-59355	In versions of Spring Authorization Server 1.5.0 through 1.5.7, the authorization endpoint performs insufficient validation of the request_uri parameter. An attacker can craft a request containing an invalid request_uri paired with an unvalidated redirect_uri, which can result in an open redirect to an attacker-controlled site.	6.1	More Details
CVE-2026-25250	EAZ EazyFix 12.9 allows a Security Feature Bypass related to a "Missing Cryptographic Step" associated with "Secure Boot disable."	6.0	More Details
CVE-2026-80206	NLTK before 3.10.3 contains a regular expression denial of service (ReDoS) vulnerability in the tgrep module. The _tgrep_node_action function compiles user-supplied regular expressions embedded in /regex/ pattern nodes and executes them via re.search against tree node labels without any validation or timeout. An attacker who controls the tgrep pattern (e.g., via tgrep_positions() or tgrep_compile() exposed to external input) can supply a pattern that triggers catastrophic backtracking, causing indefinite CPU saturation that blocks the Python process.	5.9	More Details
CVE-2025-	IBM Concert 1.0.0 through 2.3.1 could allow a remote attacker to perform unauthorized actions using man in		More

64649	the middle techniques due to improper certificate validation.	5.9	Details
CVE-2026-79940	Dell iDRAC9, 14G versions prior to 7.00.00.182 and 15G/16G versions prior to 7.20.30.50, contains an Improper Access Control vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to gaining access to unauthorized data.	5.9	More Details
CVE-2026-82235	filebrowser through 2.63.23 fails to validate named pipes in directory archive and public download handlers, allowing attackers to trigger blocking open syscalls. Authenticated users or anonymous visitors with public share links can repeatedly request archives containing named pipes to pin server goroutines and exhaust connection resources.	5.9	More Details
CVE-2025-36290	IBM Integrated Analytics System 1.0.0.0 through 1.0.31.0 does not validate or improperly validates TLS certificate validation, which could allow an attacker to obtain sensitive information using man in the middle techniques.	5.9	More Details
CVE-2025-36271	IBM Integrated Analytics System 1.0.0.0 through 1.0.31.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information.	5.9	More Details
CVE-2026-47881	Spring Batch's FlatFileItemReader supports files where a single logical record spans multiple physical lines — for example, a CSV field that contains embedded newlines wrapped in quotes. A specially crafted input file could exploit the way the reader assembles those multi-line records to consume excessive CPU time and memory, causing the batch job to stall or run out of memory. Spring Batch 6.0.0 - 6.0.4 Spring Batch 5.2.0 - 5.2.6 Spring Batch 4.3.0 - 4.3.13	5.9	More Details
CVE-2026-76549	The UpdraftPlus: WP Backup & Migration Plugin WordPress plugin before 1.26.7 does not have CSRF checks in one of its backup management actions, which could allow attackers to make a logged in admin restore an existing backup, reverting the site's database and files to an earlier state, via a crafted link.	5.9	More Details
CVE-2026-55857	MariaDB Connector/J is used to connect applications developed in Java to MariaDB and MySQL databases. Prior to 2.7.14, 3.3.5, 3.4.3, and 3.5.9, PAM dialog authentication can be coerced into transmitting the account password over an insecure connection. The mysql_clear_password plugin is gated behind a secure transport, but the sibling PAM handler SendPamAuthPacketFactory, named dialog by the server, does not declare that requirement and inherits the default secure-required value false; older branches implement the same affected behavior in SendPamAuthPacket. A hostile or man-in-the-middle server can send an Authentication Switch Request for dialog over plain TCP, causing the driver to return the user's password in cleartext when sslMode=DISABLE and restrictedAuth=null, which is the default configuration. Properly verified TLS and local Unix sockets are not exposed to this transport vector. This issue is fixed in versions 2.7.14, 3.3.5, 3.4.3, and 3.5.9.	5.9	More Details
CVE-2026-51714	Incorrect access control in the setRoamingCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to alter roaming behavior via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	5.9	More Details
CVE-2026-59276	Several components in Spring Security compare security-sensitive values using standard string equality (String.equals()) rather than a constant-time comparison. Because String.equals() returns as soon as it finds a differing character, the time taken to reject an incorrect value is proportional to the number of leading characters that match the expected value. Spring Security 7.1.0 Spring Security 7.0.0 - 7.0.6 Spring Security 6.5.0 - 6.5.11 Spring Security 6.4.0 - 6.4.18 Spring Security 5.8.0 - 5.8.27 Spring Security 5.7.0 - 5.7.25	5.9	More Details
CVE-2026-55856	MariaDB Connector/J is used to connect applications developed in Java to MariaDB and MySQL databases. Prior to 2.7.14, 3.3.5, 3.4.3, and 3.5.9, when a Java application connects with sslMode=verify-full or sslMode=verify-ca, supplies a password, and does not configure serverSslCert or trustStore, Connector/J can accept an untrusted self-signed certificate through the fallbackToSystemTrustStore=true ephemeral trust manager and record its certFingerprint for later identity binding. The OK-packet and authentication-switch paths enforce the certificate fingerprint, but the initial-handshake path does not. HandshakeResponse.encode() can therefore build and send a mysql_clear_password response before checking certFingerprint != null && !isMitMProof(), sslMode, or whether the authentication plugin is resistant to a man-in-the-middle, and the initial path also bypasses restrictedAuth. An active man-in-the-middle or hostile server can present a self-signed certificate, claim to be MariaDB, select mysql_clear_password as the initial authentication plugin, and receive the full database password before the connection is rejected. This issue is fixed in versions 2.7.14, 3.3.5, 3.4.3, and 3.5.9.	5.9	More Details
CVE-2026-74774	Dell PowerProtect One, versions 20.1.0.0 and below, contain an Improper Certificate Validation vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Protection mechanism bypass.	5.9	More Details
CVE-2026-55854	MariaDB Connector/Node.js is used to connect applications developed on Node.js to MariaDB and MySQL databases. Prior to 3.2.4, 3.3.3, 3.4.6, and 3.5.3, MariaDB Connector/Node.js can disclose an account password when PAM dialog authentication is negotiated over an insecure transport. In lib/cmd/handshake/auth/pam-password-auth.js and lib/cmd/handshake/authentication.js, the SendPamAuthPacketFactory behavior for the server-side plugin dialog lacked the secure-transport gate applied to mysql_clear_password. With the default sslMode=DISABLE and restrictedAuth=null settings, a hostile or on-path server can send an Authentication Switch Request for dialog over plain TCP, causing the connector to return the account password in cleartext. Properly verified TLS and a local Unix socket prevent	5.9	More Details

	this path, while fingerprint-only server identity validation is not sufficient. This issue is fixed in versions 3.2.4, 3.3.3, 3.4.6, and 3.5.3.		
CVE-2026-47857	In Reactor Core, applications that use the Flux.windowTimeout operator with fairBackpressure enabled are vulnerable to a Denial of Service (DoS) condition. Reactor Core 3.8.0 - 3.8.6 Reactor Core 3.5.0 - 3.7.19 Reactor Core 3.4.41 and earlier	5.9	More Details
CVE-2026-33604	An attacker that can get Dovecot to relay a message, for example through Sieve redirect or submission relay, can use a crafted line ending in the message body to bypass the outbound protection that prevents message content from being interpreted as SMTP commands. A downstream mail server that hasn't yet fixed the SMTP smuggling vulnerability can be tricked into treating part of the message body as new SMTP commands, allowing injection of spoofed email. This is the same vulnerability class as CVE-2023-51764 and CVE-2023-51766. Where you control the receiving mail servers, ensure they reject bare carriage returns in message data. Update to non-vulnerable version. No publicly available exploits are known.	5.9	More Details
CVE-2026-59294	ResourceCacheService.getCacheName() builds the on-disk filename by appending the URI fragment verbatim, without stripping path separators or .. sequences, and passes the result to new File(resourceParentFolder, newFileName) before writing the downloaded bytes there. Spring AI 2.0.0 Spring AI 1.1.0 - 1.1.8 Spring AI 1.0.9 and earlier	5.9	More Details
CVE-2026-55858	MariaDB Connector/J is used to connect applications developed in Java to MariaDB and MySQL databases. Prior to 2.7.14, 3.3.5, 3.4.3, and 3.5.9, the connector encodes and decodes protocol text and performs client-side escaping under the assumption that the connection character set is UTF-8. The server can report a mid-session change to character_set_client through OK-packet session-state tracking, including a change caused by SET NAMES, a stored routine or trigger, server configuration, or a hostile server. If character_set_client changes to a non-UTF-8 value, the driver continues to read and write UTF-8 while the server interprets the same bytes under another encoding, causing silent data corruption and a client/server charset-confusion mismatch that can defeat byte-wise quoting or escaping. The fix accepts only utf8, utf8mb3, or utf8mb4 after initialization; any other value causes SQLException with SQLState 08000 and closes the connection. This issue is fixed in versions 2.7.14, 3.3.5, 3.4.3, and 3.5.9.	5.9	More Details
CVE-2026-55859	MariaDB Connector/R2DBC is a non-blocking MariaDB and MySQL client implemented in Java. Prior to 1.4.1, org.mariadb:r2dbc-mariadb encodes and decodes all character data under the assumption that the connection character set is UTF-8. A server can announce a mid-session change to character_set_client through the OK-packet session-state-tracking mechanism, including through SET NAMES executed by a stored routine or trigger, server configuration, or a hostile or man-in-the-middle server. If the new character set is not UTF-8, the driver continues to exchange UTF-8 while the server interprets the same bytes under a different encoding, causing silent data corruption and a client/server charset-confusion mismatch that can defeat byte-wise quoting or escaping. The fix accepts only utf8, utf8mb3, or utf8mb4 after initialization; any other value raises R2dbcNonTransientResourceException with SQLState 08000 and closes the connection. This issue is fixed in version 1.4.1.	5.9	More Details
CVE-2026-75159	An unauthenticated client that can reach a MongoDB Connector for BI deployment configured with Kerberos authentication may cause mongosqld to terminate when a crafted authentication exchange encounters a specific GSSAPI error-handling condition. This can interrupt BI Connector availability until the process restarts.	5.9	More Details
CVE-2026-80179	A flaw was found in jwcrypto. A remote attacker can send a specially crafted JSON Web Encryption (JWE) token containing numerous period delimiters. This malformed token can force the JWE.deserialize() function to allocate excessive memory, leading to a MemoryError. This issue results in a denial of service (DoS) for services that process untrusted JWE values.	5.9	More Details
CVE-2026-55860	MariaDB Connector/R2DBC is a non-blocking MariaDB and MySQL client implemented in Java. Prior to 1.4.1, org.mariadb:r2dbc-mariadb does not gate clear-text password authentication plugins on transport encryption because the AuthenticationPlugin interface has no capability for a plugin to require a secure connection. A hostile or man-in-the-middle MariaDB server can send an AuthSwitchRequest naming mysql_clear_password or dialog (PAM) over a plain-TCP unencrypted connection, and AuthenticationFlow permits ClearPasswordPluginFlow or PamPluginFlow to return the user's password as cleartext bytes on the wire. The disclosed credentials can subsequently be used to authenticate directly to the database server. This issue is fixed in version 1.4.1.	5.9	More Details
CVE-2026-40019	An unauthenticated attacker can send a truncated quoted argument to the ManageSieve login process, which makes it spin in an infinite loop consuming CPU. This can cause degradation or denial of service for Sieve script management, and repeated connections can consume all available CPU on the server. Monitor system for abnormal CPU usage and kill the offending process. Restrict network access to the ManageSieve service to trusted clients. Update to non-vulnerable version. No publicly available exploits are known.	5.9	More Details
CVE-2026-32593	Winter CMS is a content management system built on the Laravel PHP framework. In versions up to and including 1.2.12, the backend Filter widget is vulnerable to SQL injection through the numberrange scope type when that scope is configured with a conditions key, allowing an authenticated backend user to inject arbitrary SQL. The scope's filter values are interpolated into the conditions statement without parameter binding, so a user with access to a list view whose filter uses this scope and configuration can supply crafted input through the filter's AJAX handler and read arbitrary database contents. No built-in Winter CMS backend views use this scope type and configuration combination, so exploitation requires a third-party plugin to	5.9	More Details

	have registered a numberrange filter scope with a conditions key, and a vanilla installation without such plugins is not affected. This issue is fixed in version 1.2.13.		
CVE-2026-47863	In Reactor Core, applications that use the Flux.bufferTimeout operator with fairBackpressure enabled are vulnerable to a Denial of Service (DoS) condition. Reactor Core 3.8.0 - 3.8.6 Reactor Core 3.7.19 and earlier	5.9	More Details
CVE-2026-80211	FrontAccounting through 2.4.20 stores and verifies user passwords as unsalted MD5 digests. admin/users.php passes md5($_POST['password']) to add_user() and update_user_password(), admin/change_current_user_password.php does the same when a user changes their own password, the forgotten-password path in includes/current_user.inc hashes the newly generated password the same way, and authentication calls get_user_auth($loginname, md5($password)). The codebase applies no per-password salt and contains no call to password_hash(), password_verify() or any other adaptive hash, so identical passwords yield identical digests and an attacker who obtains the user table can recover plaintext passwords with precomputed lookup tables or high-rate GPU cracking.	5.9	More Details
CVE-2026-40205	An attacker that holds an OAuth2 token granting only part of the required scopes can authenticate, because when more than one scope is required in the configuration, the remote token validation paths accept a token that carries only one of them, while the local token validation path correctly requires all of them. The configured authorization policy is not enforced, so a token that was granted only part of the required permissions is accepted where it should have been rejected. Use local token validation where tokens can be validated locally. Update to non-vulnerable version. No publicly available exploits are known.	5.9	More Details
CVE-2026-51739	Incorrect access control in the CloudSrvVersionCheck function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to trigger cloud update checks via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	5.9	More Details
CVE-2026-51712	Incorrect access control in the setApWiFiSchCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to alter wireless availability windows via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	5.9	More Details
CVE-2026-59287	Spring for GraphQL is vulnerable to Denial of Service attacks when using the WebSocket client with keepAlive enabled. Spring for GraphQL 2.0.0 - 2.0.4 Spring for GraphQL 1.4.0 - 1.4.6 Spring for GraphQL 1.3.0 - 1.3.9	5.9	More Details
CVE-2026-79939	Dell PowerProtect Cyber Recovery, versions Prior to 20.3, contain an UNIX Symbolic Link (Symlink) Following vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Script injection.	5.8	More Details
CVE-2026-82477	In MITRE SAF Heimdall 2.11.6 through 2.13.x before 2.14.0, an SSRF issue allows remote attackers to access internal network resources via the Tenable proxy endpoint. This occurs in apps/backend/src/tenable/tenable.controller.ts.	5.8	More Details
CVE-2026-82233	SiYuan before v3.8.1 contains a path traversal vulnerability in the asset.upload MCP tool that accepts arbitrary absolute file paths without workspace boundary validation. Attackers can induce the AI Agent to upload sensitive files such as SSH keys or credentials from outside the workspace into the asset directory through prompt injection.	5.7	More Details
CVE-2026-73102	RustDesk versions 1.3.9 through 1.4.9 contain a path traversal vulnerability in the macOS clipboard file-paste code path. The application accepts peer-supplied file descriptor names and joins them to the selected target directory without requiring normalized relative paths. A remote peer in an active clipboard file-paste session can use parent-directory components or absolute paths to write files outside the intended target directory at locations writable by the RustDesk process. Commit 6f1eb16 fixes the issue by validating descriptor names and safely joining paths.	5.7	More Details
CVE-2026-47878	DefaultExecutionContextSerializer, used by default in Spring Batch's JDBC job repository, passes Base64-decoded bytes directly to ObjectInputStream.readObject() without an ObjectInputFilter that restricts types to a trusted class allowlist. Spring Batch 6.0.0 - 6.0.4 Spring Batch 5.2.6 and earlier	5.6	More Details
CVE-2026-81530	A weakness in the client-side encryption configuration surface of the MongoDB C# Driver causes sensitive key-management credential material supplied by the application to be reproduced verbatim in the driver's human-readable diagnostic representation of its client settings, instead of being masked as other secret fields are. A party able to read the application's logs, diagnostic output, or a process memory dump may thereby recover the plaintext credentials and use them to decrypt protected field data.	5.6	More Details
CVE-2026-47875	Applications that deserialize execution contexts with Jackson2ExecutionContextStringSerializer are vulnerable to a deserialization attack if they use an untrusted data source for the job repository. The JobParameterDeserializer does not properly enforce the trusted-types allowlist, allowing an attacker to craft malicious input that can lead to arbitrary code execution, including known Jackson RCE gadgets. Spring Batch 6.0.0 - 6.0.4 Spring Batch 5.2.0 - 5.2.6	5.6	More Details
CVE-2026-82640	browser-use web-ui versions 2.0.0 through 3.0.0 write configured LLM API keys to disk in cleartext without encryption or access restrictions. Attackers with read access to the temporary settings directory can recover provider API keys from predictably-named JSON files.	5.5	More Details
	A flaw was found in libsolv, a dependency-resolution library used by RPM-based package managers such as		

CVE-2026-82327	dnf and zypper to work with .solv repository cache files. When libsolv rewrites a .solv cache file, it reads directory-id values from the file's compressed filelist data without validating that they fall within the expected range. A corrupted or specially crafted .solv cache file (for example, one left in a torn state after an unclean system shutdown) can cause an out-of-bounds memory write when a tool such as dnf, yum, or zypper next processes it. Successful exploitation is expected to result in a crash of the affected tool (denial of service); it is not expected to allow arbitrary code execution because the out-of-bounds write always stores a fixed, non-attacker-controlled value.	5.5	More Details
CVE-2026-34616	DNG SDK versions 1.7.1 2502 and earlier are affected by an out-of-bounds read vulnerability that could lead to memory exposure. An attacker could leverage this vulnerability to disclose sensitive information from memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-34620	DNG SDK versions 1.7.1 2502 and earlier are affected by an out-of-bounds write vulnerability that could lead to application denial-of-service. An attacker could leverage this vulnerability to corrupt memory, causing the application to crash or become unresponsive. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-81835	A security vulnerability has been detected in RooCodeInc Roo-Code up to 3.51.1. This affects the function fetch_instructions of the file malicious_mcp_server.py of the component MCP Integration Trust Model. The manipulation leads to code injection. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used. Multiple isses were reported to the vendor beforehand. They explain, that "they all apply to Roo Code, a project we no longer support - the repository was archived a while ago, and we don't encourage anyone to use it." This vulnerability only affects products that are no longer supported by the maintainer.	5.5	More Details
CVE-2026-82875	ToolJet before v3.16.208 contains an authorization bypass vulnerability in TooljetDB controller endpoints that accept organizationId from URL path without verifying it matches the authenticated user's workspace. Authenticated users can enumerate, create, rename, and delete TooljetDB tables in any other workspace by manipulating the organizationId parameter in requests.	5.5	More Details
CVE-2026-82181	Medical Practice Management System developed by Le-yan has a Sensitive Data in URL vulnerability. Unauthenticated remote attackers can obtain sensitive information via victim's browser history or log files.	5.5	More Details
CVE-2026-81687	openssl_encrypt versions before 1.4.9 fail to enforce a time ceiling on key derivation function iteration counts specified in file metadata. Attackers can craft files with extremely high KDF iteration counts to consume CPU resources for unbounded periods before password verification occurs.	5.5	More Details
CVE-2026-80158	A flaw was found in the ipa_getkeytab module of the community.general Ansible collection. The module's bind_pw parameter, used to supply the LDAP simple-bind password when retrieving a Kerberos keytab, is not declared with no_log, unlike the sibling password parameter in the same module. As a consequence, the supplied IPA/LDAP bind password is recorded in cleartext in the managed host's system journal/syslog (the module's "Invoked with" record), is included in the module's return values and verbose (-v) output, and is displayed in Automation Controller / AWX job output. The password is additionally passed on the command line to the ipa-getkeytab helper (as --bindpw <value>), exposing it in the process list to local users while the command runs. An attacker able to read these logs, job output, or the process table can obtain the directory bind credential, potentially compromising the accounts and objects that credential can access.	5.5	More Details
CVE-2026-81703	openssl_encrypt versions before 1.4.9 fail to validate encryption status of embedded post-quantum private keys in file metadata. Attackers can craft files with unencrypted embedded PQC keys that decrypt under any password, bypassing authentication and producing attacker-chosen plaintext with false integrity verification.	5.5	More Details
CVE-2026-79902	A flaw was found in the Seattle FilmWorks plugin in GIMP. When processing a specially crafted SFW image file, the plugin allocates a Variable-Length Array (VLA) on the stack without integer overflow checks, causing an unbounded stack allocation. This issue leads to an application crash, resulting in a denial of service.	5.5	More Details
CVE-2026-81833	A security flaw has been discovered in RooCodeInc Roo-Code up to 3.51.1. Affected by this vulnerability is the function optimizeQuery of the file src/utils/helpers.ts of the component CodeIndexManager. Performing a manipulation results in code injection. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks. Multiple isses were reported to the vendor beforehand. They explain, that "they all apply to Roo Code, a project we no longer support - the repository was archived a while ago, and we don't encourage anyone to use it." This vulnerability only affects products that are no longer supported by the maintainer.	5.5	More Details
CVE-2026-3035	GitLab has remediated an issue in GitLab EE affecting all versions from 11.3 before 19.1.7, 19.2 before 19.2.5, and 19.3 before 19.3.1 that, under certain conditions, an authenticated user with project Maintainer permissions could have accessed the terminal of a protected environment they were not authorized to use due to improper authorization checks.	5.5	More Details
CVE-2026-81697	openssl_encrypt (pip package openssl-encrypt) versions <= 1.4.8 contain a CWD-relative configuration file resolution flaw in crypt_settings.py, where CONFIG_FILE (originally the absolute per-user path ~/.crypt_settings.json) is reassigned at line 84 to the bare relative name 'crypt_settings.json'. As a result, the legacy Tk GUI's SettingsTab reads and writes KDF settings from crypt_settings.json in the process launch (current working) directory instead of the user's home directory. An attacker who plants a malicious crypt_settings.json (e.g. sha256:1 with all memory-hard KDFs disabled) can silently downgrade encryption	5.5	More Details

	performed in that GUI session to roughly one hash round, bypassing the weak-KDF preflight and enabling offline brute-force attacks against the resulting ciphertext. Fixed in 1.4.9.		
CVE-2026-82797	Uncontrolled Recursion vulnerability in Samsung Open Source rlottie allows Serialized Data with Nested Payloads. This issue affects rlottie: before 8de0d9e6ca80ffef654965505981727b9fa06a51.	5.5	More Details
CVE-2026-81847	A vulnerability was found in MAA-AI MaaMCP up to 1.1.1.dev6+g2e4a41287. The affected element is the function save_pipeline/load_pipeline of the file pipeline_tools.py. Performing a manipulation results in path traversal. The attack can be initiated remotely. The exploit has been made public and could be used. The patch is named c93ef45cba75295eba26d9ff1ffb9202a91c6150. To fix this issue, it is recommended to deploy a patch.	5.5	More Details
CVE-2026-47880	A producer who can publish to a JMS destination consumed by any Spring Integration JMS inbound component can set String JMS properties named replyChannel, errorChannel, or json__TypeId__ which are copied verbatim into the Spring Integration MessageHeaders. Spring Integration 7.1.0 Spring Integration 7.0.0 - 7.0.5 Spring Integration 6.5.0 - 6.5.10 Spring Integration 6.4.0 - 6.4.12 Spring Integration 5.5.21 and earlier	5.4	More Details
CVE-2026-38725	xipblog module v2.0.1 and before for PrestaShop allows unauthenticated remote attackers to inject arbitrary JavaScript via the name and content parameters in ajax.php. The input is stored in the database without HTML sanitization and rendered in Smarty templates without output escaping, resulting in Stored Cross-Site Scripting (XSS). When an administrator reviews comments in the back office, the payload executes with admin-level session context, leading to full store compromise.	5.4	More Details
CVE-2026-4378	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Akilli Ticaret Software Technologies Ltd. E-Commerce Pack allows Stored XSS. This issue affects E-Commerce Pack: from 4.5.001 through 28082026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.4	More Details
CVE-2026-13481	The IEEE 1588 PTP management-message parser in subsys/net/lib/ptp/tlv.c mishandles the PTP_MGMT_TIME management id. In tlv_mgmt_post_recv(), the PTP_MGMT_TIME case casts mgmt_tlv->data to a 10-byte struct ptp_timestamp and reads it (then byte-swaps and writes it back) without first checking that the TLV data field is at least sizeof(struct ptp_timestamp). Every sibling management id in the same switch validates its length first; PTP_MGMT_TIME was the only case lacking that check. The length passed in is the management data size (tlv->length - 2), and the upstream guard in ptp_tlv_post_recv() only requires tlv->length > 2, while msg_tlv_post_recv() validates only that the TLV fits within the received byte count, not a per-id minimum. A peer on the local PTP segment can therefore send a PTP_MSG_MANAGEMENT message carrying a short PTP_MGMT_TIME TLV (data as small as 2 bytes), causing the parser to read and write 8 bytes beyond the validated data. The message type and TLV contents are taken straight off the wire, so the path is reachable by any adjacent attacker when CONFIG_PTP is enabled. The over-read and write-back stay within the struct ptp_msg allocation (mgmt_tlv->data lives in the leading mtu[NET_ETH_MTU] union member, so data + 10 lands at most a few bytes past mtu[], inside the same object), so this is an out-of-bounds read of adjacent in-object memory plus a bounded in-place corruption of the message's parsed timestamp, not past-allocation memory corruption. Impact is limited to minor information exposure of adjacent bytes and corruption of the device's parsed management TIME value; there is no crash on the access and no reachable reference-count corruption. The fix adds if (length < sizeof(struct ptp_timestamp)) { return -EBADMSG; } before the cast, matching the other management-id cases and fully closing the receive-path defect.	5.4	More Details
CVE-2026-82660	Nodemailer before 8.0.9 fails to enforce disableFileAccess and disableUrlAccess options during message normalization in jsonTransport. Attackers can read local files or fetch URLs by supplying path or href values in message content fields, bypassing intended access controls.	5.4	More Details
CVE-2026-82661	Nodemailer before 8.0.9 fails to sanitize carriage return and line feed characters in list comment fields, allowing attackers to inject arbitrary message headers. An attacker with control over list.*.comment parameters can inject CRLF sequences to create additional headers in generated RFC822 messages, altering mail client behavior and message semantics.	5.4	More Details
CVE-2026-54553	Starlette-Admin is a fast, beautiful and extensible administrative interface framework for FastAPI and Starlette applications. Prior to 0.16.1, the list API does not validate user-supplied order_by and structured where field names against the configured sortable_fields and searchable_fields allowlists. An authenticated user with access to an affected list endpoint can submit arbitrary field names to starlette_admin/base.py and the BaseModelView validation path, bypassing restrictions presented by the administrative user interface. Requests can sort or filter on fields that are not intended to be sortable or searchable, causing limited information exposure. Invalid field names and special Python attribute names such as metadata and the class dunder attribute can also trigger unhandled exceptions and HTTP 500 responses, causing limited denial of service for targeted requests. This issue is fixed in version 0.16.1.	5.4	More Details
CVE-2026-40464	NSP is vulnerable to a stored XSS due to insufficient validation or encoding of user-controlled input in a workflow application. An authenticated attacker with access to the workflow application could embed harmful code that runs when another user views the content.	5.4	More Details
	The Grav API plugin (getgrav/grav-plugin-api) before 1.0.18 does not apply the API-key scope cap in the injectSecurityTab() function of BlueprintController when deciding whether a page's security/permissions		

CVE-2026-80204	blueprint section is editable. Because the function performs raw isSuperAdmin()/hasPermission() checks without a request parameter, it cannot enforce scopeAllows(). A caller holding a scoped API key may therefore see (and potentially edit) page permission fields beyond the scope granted to the key. The end-to-end write-time impact was not fully confirmed by the reporter.	5.4	More Details
CVE-2026-47859	RFC6587SyslogDeserializer, used by the Spring Integration syslog TCP inbound adapter to decode RFC 6587 / RFC 5424 frames, trusts the sender-supplied octet count of an octet-counted frame and allocates a byte array of exactly that size with no upper bound. Spring Integration 7.1.0 Spring Integration 7.0.0 - 7.0.5 Spring Integration 6.5.0 - 6.5.10 Spring Integration 6.4.0 - 6.4.12 Spring Integration 5.5.21 and earlier	5.4	More Details
CVE-2026-81759	Contributor Broken Access Control in WpEvently <= 5.5.0 versions.	5.4	More Details
CVE-2026-18393	A flaw was found in FFmpeg. The tdsc_load_cursor() function writes beyond the bounds of a heap-allocated buffer when processing crafted TDSC cursor data. A remote attacker could exploit this by supplying a specially crafted video file, potentially leading to a denial of service or arbitrary code execution.	5.4	More Details
CVE-2026-81279	Subscriber Broken Access Control in Push Notification for Post and BuddyPress <= 3.20 versions.	5.4	More Details
CVE-2026-39071	WordPress plugin (Spiffy Plugin) before 5.0.9 is affected by Stored Cross-Site Scripting in Event Title field. An authenticated attacker with the lowest privileged role (contributor) can exploit this to redirect user to malicious site or control the account.	5.4	More Details
CVE-2026-81668	A flaw was found in Katello where the Content View Filter Rules API does not properly enforce authorization on the parent Content View Filter. An authenticated, low-privileged user with Content View permissions in one organization may be able to access and modify filter rules belonging to a Content View Filter in another organization by supplying that filter's identifier. This can result in unauthorized disclosure of filter-rule information and unauthorized changes to unpublished Content View filter configuration.	5.4	More Details
CVE-2026-82599	A vulnerability was identified in SeaCMS up to 13.6. Affected by this vulnerability is the function unlink of the file /member.php?action=chgpwdsubmit of the component Avatar Upload. Such manipulation of the argument oldpic leads to path traversal. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	5.4	More Details
CVE-2026-82603	A vulnerability was detected in SeaCMS up to 13.6. This issue affects some unknown processing of the file /member.php?action=del_pl of the component Comment Cache. The manipulation of the argument itype/vid results in path traversal. The attack may be launched remotely. The exploit is now public and may be used.	5.4	More Details
CVE-2026-82423	A vulnerability has been found in macrozheng mall up to 1.0.3. The affected element is an unknown function of the file /order/paySuccess of the component Payment Status Endpoint. The manipulation of the argument orderId leads to enforcement of behavioral workflow. The attack is possible to be carried out remotely. The vendor deleted the GitHub issue for this vulnerability without any explanation.	5.4	More Details
CVE-2026-45694	LibreNMS is a network monitoring system. In versions up to and including 26.4.0, the Proxmox application view is vulnerable to reflected cross-site scripting through the user-supplied instance and vmid GET parameters, which are reflected into the page title without adequate encoding. The parameters are placed into the page title with only strip_tags applied, and the title is then written into an inline document.title assignment through string interpolation, so a single quote terminates the JavaScript string and the remaining input runs as script. An attacker who lures an authenticated user into following a crafted link can execute script in that user's session, enabling actions such as theft of session data. This issue is fixed in version 26.5.0.	5.4	More Details
CVE-2026-47862	An attacker who can set the file_name header on a message reaching a ZipTransformer with ZipResultType.FILE (the default) can cause the resulting .zip archive to be written to an arbitrary filesystem path outside the configured workDirectory. Spring Integration 7.1.0 Spring Integration 7.0.0 - 7.0.5 Spring Integration 6.5.0 - 6.5.10 Spring Integration 6.4.0 - 6.4.12	5.4	More Details
CVE-2026-75802	AjaxEditableChoiceLabel in wicket-extensions, when constructed with a non-null IChoiceRenderer, writes the display value obtained from that renderer into the label's markup without applying the HTML escaping Wicket performs by default for component model values. An attacker who can influence the choice or model data rendered by such a label can inject HTML or script that executes in the browser of any user who views the page. The same value is correctly escaped when the component's dropdown editor renders it as an option, so only the label rendering is affected. AjaxEditableLabel, AjaxEditableChoiceLabel and AjaxEditableMultiLineLabel write the value returned by the protected defaultNullLabel() method into the label's markup the same way when the component's model is empty, while the model value they show otherwise is escaped. The default implementation returns a constant, so an application is affected where it overrides that method and returns a value an attacker can influence. Neither value could be escaped by configuration, because escapeModelStrings had no effect on any of the three components: it is read by the label they render with rather than by the component itself, and nothing carried the setting across. This issue affects Apache Wicket: from 8.0.0 through 8.18.0, from 9.0.0 through 9.23.0, from 10.0.0 through 10.10.0. Older, unsupported releases are also affected; the display value from the renderer since 6.22.0 and the null label since 1.4.0. Users are recommended to upgrade to version 8.19.0, 9.24.0 or 10.11.0, which fix the issue.	5.4	More Details

CVE-2026-76982	Improper neutralization of input during web page generation in Apache Wicket. org.apache.wicket.markup.html.form.Button clears the escape-model-strings flag in its constructor, so that the value attribute it writes is not encoded twice — ComponentTag already encodes attribute values when it writes the tag. That reasoning holds only for the attribute. When the component is attached to a <button> element rather than an <input>, it writes its model object into the element body instead, and nothing encodes an element body, so markup in the model is rendered as markup. An application is affected where it renders a Button on a <button> element and that button's model holds data an attacker can influence. Wicket cannot determine where a model value comes from, so whether it reaches the page from a request or from storage is a property of the application. The subclasses that inherit this constructor — AjaxButton, AjaxFallbackButton and WizardButton — are affected on the same terms. As a workaround, calling setEscapeModelStrings(true) on a button that renders as a <button> element escapes the body correctly, and does not cause double encoding, because the value attribute is written only for <input> elements. This issue affects Apache Wicket: from 8.0.0 through 8.18.0, from 9.0.0 through 9.23.0, from 10.0.0 through 10.10.0. Older, unsupported releases from 6.25.0 and 7.5.0 onwards are also affected. Users are recommended to upgrade to version 8.19.0, 9.24.0 or 10.11.0, which fix the issue.	5.4	More Details
CVE-2026-51703	Incorrect access control in the setWiFiScheduleCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to alter when Wi-Fi is available via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	5.4	More Details
CVE-2026-82469	Rodauth before 2.47.0 contains an authentication bypass vulnerability in the jwt_refresh route that issues new JWT access tokens without requiring a refresh token. Attackers can present an access token to the refresh route via non-POST methods to obtain a new valid access token, enabling indefinite account access with temporary token possession.	5.4	More Details
CVE-2026-14368	The LwM2M JSON content formatter's get_string() in subsys/net/lib/lwm2m/lwm2m_rw_json.c copies a parsed JSON string into a caller-supplied buffer and NUL-terminates it. The length guard used if (string_length > buflen), which accepts a string whose length is exactly buflen. After memcpy() fills the whole buffer, buf[string_length] = '\0' then writes one byte past the end of the buffer (CWE-787). The string value and its length are taken directly from the incoming CoAP payload during a LwM2M WRITE: do_write_op_json() parses the payload obtained from coap_packet_get_payload(), and get_string() is invoked from lwm2m_write_handler() (engine_get_string() in subsys/net/lib/lwm2m/lwm2m_message_handling.c) for a LWM2M_RES_TYPE_STRING resource. The destination buf/buflen is either the resource instance's fixed data buffer (res_inst->data_ptr/max_data_len) or the engine validation buffer (msg->ctx->validate_buf). A LwM2M server (the client's DTLS peer) can therefore write a string resource with a value whose length equals the target buffer size and force a one-byte overflow. The overflow is a single out-of-bounds write of the constant byte 0x00 immediately past the resource or validation buffer, corrupting the adjacent byte in memory. It is not an information leak and the written value is fixed, so it is not a direct code-execution primitive, but it can corrupt adjacent state (an adjacent resource value, a length/flag field, or a struct field) and cause data corruption or a crash. Triggering the write is deterministic; the resulting impact depends on memory layout. The fix changes the guard to string_length >= buflen, rejecting the exact-length case and aligning the JSON formatter with the other content formatters (lwm2m_rw_plain_text.c, lwm2m_rw_oma_tlv.c, lwm2m_rw_senml_json.c, lwm2m_rw_cbor.c, lwm2m_rw_senml_cbor.c), which already used the correct boundary check.	5.4	More Details
CVE-2026-76983	Improper neutralization of input during web page generation in Apache Wicket. The <wicket:label> tag is provided by org.apache.wicket.markup.html.form.AutoLabelTextResolver, which is registered by default in every WebApplication. The resolver writes the label it finds into the markup as it is, and reads no escaping setting at all, so markup in a label is rendered as markup. When the label comes from the labelled component's label model, set through FormComponent#setLabel(IModel), it is written to the markup unescaped. An application is affected where the label of a form component holds data an attacker can influence. Wicket cannot determine where a model value comes from, so whether it reaches the page from a request or from storage is a property of the application. There is no workaround. Unlike every other rendering path in Wicket, the resolver never consulted the escape-model-strings setting, so an application had no way to ask for the label to be escaped. The body of a <wicket:label> tag is markup by design and is not affected; it remains the supported way to place markup in a label. This issue affects Apache Wicket: from 8.0.0 through 8.18.0, from 9.0.0 through 9.23.0, from 10.0.0 through 10.10.0. Older, unsupported releases from 1.5.0 onwards are also affected. Users are recommended to upgrade to version 8.19.0, 9.24.0 or 10.11.0, which fix the issue.	5.4	More Details
CVE-2026-76984	Improper neutralization of input during web page generation in Apache Wicket. org.apache.wicket.markup.head.MetaDataHeaderItem generates <meta> and <link> header tags. It escaped the attribute names it wrote, but ran the attribute values through a replacement of " with \". A backslash before a double quote means nothing in HTML, so a value containing a double quote ends its own attribute and what follows is parsed as further attributes of the generated tag. An application is affected where it supplies an attribute value holding data an attacker can influence, through addTagAttribute or the forMetaTag and forLinkTag factory methods. A value may be given as an IModel, so it is not necessarily a literal. There is no setting to change; an application can only avoid supplying a value that contains a double quote. Note that these values have never been escaped effectively: before the change released in 6.24.0, 7.4.0 and 8.0.0 they were written with no escaping at all. This issue affects Apache Wicket: from 8.0.0 through 8.18.0, from 9.0.0 through 9.23.0, from 10.0.0 through 10.10.0. Older, unsupported releases from 6.17.0 onwards are also affected. Users are recommended to upgrade to version 8.19.0, 9.24.0 or 10.11.0, which fix the issue.	5.4	More Details

CVE-2026-62904	Incorrect authorization in Microsoft Edge (Chromium-based) allows an unauthorized attacker to disclose information over a network.	5.4	More Details
CVE-2026-66323	Improper neutralization of parameter/argument delimiters in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	5.4	More Details
CVE-2026-70309	Origin validation error in Microsoft Edge (Chromium-based) allows an unauthorized attacker to bypass a security feature over a network.	5.4	More Details
CVE-2026-82835	A weakness has been identified in caoqianming django-vue-admin 1.0. This vulnerability affects unknown code of the file /api/file/. Executing a manipulation of the argument file_id can lead to improper access controls. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	5.4	More Details
CVE-2026-82834	A security flaw has been discovered in Doccano Open Source Annotation Tools for Machine Learning Practitioners and Auto Labeling Pipeline Module to Annotate a Document Automatically up to 1.8.5. This affects the function LabelList of the file /v1/projects/1/category-types of the component Bulk-Delete Endpoint. Performing a manipulation results in improper access controls. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	5.4	More Details
CVE-2026-81267	A malicious webpage could stall a popup's cross-origin navigation after commit, causing the address bar to display the destination origin while continuing to render attacker-controlled content. This vulnerability was fixed in Firefox for iOS 155.0.	5.4	More Details
CVE-2026-81524	A weakness in the MongoDB C Driver allows special elements in caller-supplied database and collection name components to pass without sanitization when the driver composes the target namespace for an operation. An application that incorporates untrusted input into these name components can have operations directed at a resource other than the one intended.	5.4	More Details
CVE-2026-81528	A MongoDB C# driver document-replacement code path omits the element-name/shape validation that the equivalent write paths apply, so a value supplied as a replacement is forwarded to the server without neutralization of query-language special elements. An application that passes untrusted, loosely-typed input as a replacement value therefore allows that input to be interpreted by the database as update logic rather than as data, executing under the application's own database credentials. Applications using strongly-typed document mappings are not affected.	5.4	More Details
CVE-2026-82811	A security vulnerability has been detected in Toggl OÜ Toggl Track Extension 4.11.16. This affects an unknown function of the component postMessage Handler. The manipulation leads to origin validation error. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.4	More Details
CVE-2026-82813	A vulnerability was detected in BEN Group TubeBuddy for YouTube Extension up to 5.8.4 on Chrome. This impacts the function TBGlobal.GetToken of the file tubebuddymaster1.js. The manipulation of the argument t/c/r results in insufficient verification of data authenticity. It is possible to launch the attack remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure.	5.4	More Details
CVE-2026-70331	Improper neutralization of input used for llm prompting in Microsoft Edge for iOS allows an unauthorized attacker to perform spoofing over a network.	5.4	More Details
CVE-2026-74929	The Project Manager WordPress plugin before 4.0.7 does not restrict several of its REST API routes to the projects a user belongs to, allowing any authenticated user, such as a subscriber, to read other projects' task content and user email addresses and to modify other projects' task boards.	5.4	More Details
CVE-2026-81731	Frappe 15.11.0 through 16.32.0 stores and renders the workspace card description without XSS filtering. The description field of the Workspace Link doctype is declared with "ignore_xss_filter": 1 in frappe/desk/doctype/workspace_link/workspace_link.json, and _sanitize_content() in frappe/model/base_document.py skips any field carrying that flag, so the value is stored exactly as submitted. frappe.desk.desktop.get_desktop_page returns it unchanged, and LinksWidget.set_body() in frappe/public/js/frappe/widgets/links_widget.js interpolates it into a Bootstrap popover created with html: true, by way of the __() translation helper, which performs no HTML escaping. A user holding the Workspace Manager role can therefore place arbitrary markup in a public workspace's card description and have it execute in the session of any desk user who opens that workspace and hovers the description, including higher-privileged users, allowing session token theft and authenticated requests as the victim. The flag is removed on the development branch but remains present in the shipped 15.x and 16.x release lines, so no released version carries the fix.	5.4	More Details
CVE-2026-77757	The Directorist: AI-Powered Business Directory, Listings & Classified Ads WordPress plugin before 8.9.3 does not sanitize a user-supplied image reference before using it as the source of a file move, allowing users with a subscriber-level account to relocate arbitrary server-readable image files into a publicly accessible directory, and to delete them from their original location.	5.4	More Details
	Improper neutralization of input during web page generation in Apache Wicket. org.apache.wicket.extensions.markup.html.form.palette.component.AbstractOptions, which renders the two		

CVE-2026-76985	option lists of a Palette, escapes the id and the display value of each option according to the escape-model-strings setting, and wrote the attribute names and values returned by getAdditionalAttributes into the <option> tag as they came. An application is affected where it overrides Palette.getAdditionalAttributesForChoices, Palette.getAdditionalAttributesForSelection or AbstractOptions.getAdditionalAttributes and returns a value holding data an attacker can influence. These methods return null by default, so an application that does not override them is not affected. As a workaround, escape the values in the override. This issue affects Apache Wicket: from 8.0.0 through 8.18.0, from 9.0.0 through 9.23.0, from 10.0.0 through 10.10.0. Older, unsupported releases from 1.4.0 onwards are also affected. Users are recommended to upgrade to version 8.19.0, 9.24.0 or 10.11.0, which fix the issue.	5.4	More Details
CVE-2026-54256	Winter CMS is a content management system built on the Laravel PHP framework. In versions up to and including 1.2.12, the backend FileUpload form widget trusted an attacker-controlled file_id POST parameter when resolving the attachment it operates on, allowing an authenticated backend user to read and modify attachment records belonging to other users or records. The widget's getFileRecord() lookup resolved the posted id against the global system_files table without verifying that the file belonged to the widget's own relation, parent record, or deferred-binding session. Because all attachments share a single File model and table and attachment ids are sequential integers that are easily enumerated, a user reaching any form with a fileupload field, including the built-in My Account avatar field that requires no specific permission, could target arbitrary attachments to modify their title and description via onSaveAttachmentConfig and change their sort order via onSortAttachments, which passed posted ids straight to an unscoped update. CSRF tokens remain enforced, so exploitation requires a valid authenticated backend session with any level of access. This issue is fixed in version 1.2.13.	5.4	More Details
CVE-2026-55779	Silverstripe Versioned provides versioning for Silverstripe models. Prior to 3.2.1, RestoreAction::getRestoreMessage() in src/RestoreAction.php builds ArchiveAdmin restore notifications rendered as CAST_HTML and inserts $restoredItem->Title, $restoredItem->URLSegment, $restoredItem->CMSEditLink(), and $changedProperty['value'] without applying Convert::raw2xml(). When an administrator restores an archived page containing a crafted title or URL segment, the generated restoration message can execute stored JavaScript in the administrator's browser, compromising the confidentiality and integrity of the CMS session. This issue is fixed in version 3.2.1.	5.4	More Details
CVE-2026-17522	The Newsletters WordPress plugin before 4.17 does not perform any nonce or capability check when saving one of its settings screens, and writes every submitted parameter into its own options, allowing attackers to make a logged in administrator overwrite arbitrary Newsletters WordPress plugin before 4.17 settings, including the credential protecting its API, via a Cross-Site Request Forgery attack.	5.4	More Details
CVE-2026-71402	An out-of-bounds read was found in the DHCPv4 packet capture code of wicked. ni_capture_inspect_udp_header() in src/capture.c reports the IP total length as the payload length instead of the length of the remaining UDP payload. Consequently, the DHCP option walker in the DHCPv4 client (wickedd-dhcp4) reads up to ihl + 8 bytes — at most 68 bytes — past the end of the 1500-byte packet receive buffer. An unauthenticated attacker on the same network who sends a crafted DHCP/UDP packet can make the client parse adjacent heap memory as DHCP options, so that heap contents such as allocator metadata or pointer values can be interpreted into lease fields. The over-read is bounded to 68 bytes; no memory write, no attacker control over the adjacent bytes and no remote exfiltration primitive has been demonstrated. This issue affects wicked up to and including version 0.6.80.	5.4	More Details
CVE-2026-71396	Bendix EC80 Brake ECU uses hard-coded credentials, which could allow an attacker to disable automatic traction control.	5.4	More Details
CVE-2026-82881	Aix-DB through 1.2.4 renders markdown with raw HTML enabled into v-html bindings without sanitization, allowing stored cross-site scripting attacks. Attackers can inject malicious HTML and JavaScript through markdown content in chat responses, skill descriptions, or knowledge messages that execute in users' browsers when viewed.	5.4	More Details
CVE-2026-81278	Missing Authorization vulnerability in WPExperts Post SMTP allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Post SMTP: from 4.0.0 through beta.1.	5.4	More Details
CVE-2026-75548	The affected Ebyte device web management interface does not restrict the interface from being rendered within an external frame. An unauthenticated remote attacker could use a crafted webpage to mislead an authenticated administrator into initiating unintended configuration changes or disruptive actions.	5.4	More Details
CVE-2026-82267	Komodo through 2.3.2 discloses internal resource identifiers and writes audit entries before performing permission checks in the /execute and /execute/{variant} handlers. Authenticated users can guess resource names to obtain internal identifiers and insert fraudulent audit log entries misrepresenting privileged operations.	5.4	More Details
CVE-2026-80195	Kimai before 2.63.0 contains a business logic / improper authorization vulnerability in the team update API endpoint (PATCH /api/teams/{id}), which removes all existing team members before validating the submitted replacement member list. An authenticated teamlead (or other user) with permission to edit a team can submit a malformed members payload; although Kimai returns a validation error, the existing membership rows have already been deleted. This bypasses the dedicated member-removal endpoint's protection against removing teamleaders and can leave a team with no members or teamleaders, disrupting team-based access control.	5.4	More Details

CVE-2026-82470	Rodauth before 2.47.0 contains a time-based one-time password reuse vulnerability in the otp feature that fails to track the last accepted code timestamp. Attackers who observe a valid TOTP code can replay it during the drift window to bypass the second authentication factor.	5.4	More Details
CVE-2026-51153	Stored Cross-Site Scripting (XSS) in TaskRunHandler.post() in web/handlers/task.py in QD 20220208 through 20250803. When a task is run via /task/<taskid>/run, the handler renders task log content (logtmp) into the HTML response using Python % string formatting without HTML encoding. logtmp is populated from the exception object or from new_env.variables.__log__, which is attacker-controlled via the template extract_variables mechanism. A low-privileged authenticated attacker can create a crafted HAR template that extracts arbitrary HTML/JavaScript into the __log__ variable via the api://util/unicode endpoint. When a victim triggers the task run, the embedded script executes in the victim browser within the QD application context.	5.4	More Details
CVE-2026-82465	pac4j-saml before 6.5.6 does not require signature validation of SAML LogoutRequest messages in SAML2LogoutValidator.validateLogoutRequest(). When an IdP sends no SessionIndex, a session can be destroyed based solely on the NameID, allowing an unauthenticated attacker to submit an unsigned LogoutRequest with a guessed identifier (e.g., an email address used as NameID) to terminate a victim's SAML session.	5.3	More Details
CVE-2026-82652	SiYuan before v3.8.1 fails to filter invisible-tier content from SQL embed blocks, attribute-view keys, and attribute-view backlinks in publish mode. Anonymous readers can enumerate invisible content through these three listing mechanisms despite admin configuration marking content unlisted.	5.3	More Details
CVE-2026-82276	StarRocks through 4.0.13 contains an authentication bypass vulnerability in five REST handler classes that override execute() directly instead of implementing executeWithoutPassword(). Attackers can access six unauthenticated endpoints on the frontend HTTP port to disclose cluster topology, database metadata, JVM statistics, and version information without credentials.	5.3	More Details
CVE-2026-81274	Subscriber Broken Access Control in Ditty <= 3.1.67 versions.	5.3	More Details
CVE-2026-67275	Dell PowerProtect One, versions 20.1.0.0 and below, contain a Reliance on Insufficiently Trustworthy Component vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Cache poisoning.	5.3	More Details
CVE-2026-13172	The Eventin WordPress plugin before 4.1.22 does not restrict access to non-published content by status or ownership in one of its REST API namespaces, allowing unauthenticated users to retrieve draft, pending and private posts belonging to other users, along with the passwords and contents of password-protected ones.	5.3	More Details
CVE-2026-81664	The OpenFaaS gateway registers GET /system/telemetry in gateway/main.go and, when basic_auth is enabled, wraps each administrative /system/* handler in auth.DecorateWithBasicAuth. TelemetryHandler was left out of that wrap block from 0.27.11, which introduced the route, until 0.27.14, which added it. On an affected gateway the route therefore reaches the forwarding proxy with no credential check and returns whatever the configured provider serves for /system/telemetry, so any client that can reach the gateway port can read the provider's telemetry regardless of the basic_auth setting. The exposed content depends on the provider, and covers resource and invocation metrics for faasd and pod or cluster state for faas-netes.	5.3	More Details
CVE-2026-77694	The Eventin WordPress plugin before 4.1.19 does not properly restrict which changes a guest checkout token is allowed to authorise on an order, allowing unauthenticated users to mark their own unpaid order as completed and be issued a valid paid ticket with no payment taken.	5.3	More Details
CVE-2026-81486	A vulnerability was detected in bsmi021 mcp-file-context-server 1.0.0. Affected by this issue is the function read_context of the file src/index.ts of the component Path Resolution. Performing a manipulation of the argument path results in path traversal. It is possible to initiate the attack remotely. The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	5.3	More Details
CVE-2026-51727	Incorrect access control in the SystemSettings function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to retrieve administrative import and export endpoint information via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	5.3	More Details
CVE-2026-81485	A security vulnerability has been detected in danielpopamd linkedin-ads-mcp 1.0.0. Affected by this vulnerability is the function fs.readFileSync of the file src/tools/campaign-management.ts of the component Media Upload. Such manipulation of the argument filePath leads to path traversal. The attack may be performed from remote. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report but has not responded yet.	5.3	More Details
CVE-2026-82602	A security vulnerability has been detected in SeaCMS up to 13.6. This vulnerability affects unknown code of the file /ass.php. The manipulation leads to authorization bypass. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used.	5.3	More Details
CVE-2026-75798	The AI Engine WordPress plugin before 3.7.2 does not perform an authorisation check on one of its administration-only features, relying instead on a token it hands out to anonymous visitors, allowing unauthenticated attackers to run AI queries of their own choosing against the site owner's configured	5.3	More Details

	provider account.		
CVE-2026-47845	In specific scenarios, Reactor Netty HTTP Server may incorrectly evaluate the remote IP address when HAProxy Protocol is enabled. In order for this to happen, the application must be configured to use HAProxy Protocol. Reactor Netty 1.3.0 - 1.3.6 Reactor Netty 1.1.0 - 1.2.18 Reactor Netty 1.0.52 and earlier	5.3	More Details
CVE-2026-37073	Incorrect access control in /vfm-admin/ajax/sendfiles.php in Veno File Manager Project 4.4.9 allows an unauthenticated attacker to send emails from the configured SMPT server on the application via making a POST request to the endpoint with needed parameters and header.	5.3	More Details
CVE-2026-59271	When the RabbitMQ management aliveness check fails, the configured admin password is embedded in cleartext in the thrown exception message. Spring AMQP 4.1.0 Spring AMQP 4.0.0 - 4.0.4 Spring AMQP 3.2.0 - 3.2.12 Spring AMQP 2.4.18 and earlier	5.3	More Details
CVE-2026-81562	A security flaw has been discovered in AlexGladkov claude-in-mobile 3.10.2. This affects the function execSync of the file src/adb/client.ts. Performing a manipulation results in os command injection. The attack requires a local approach. The exploit has been released to the public and may be used for attacks. Upgrading to version 3.10.3 is able to mitigate this issue. The patch is named a86d9e55694c98a122943eeff859461d0b9aa6d6. It is suggested to upgrade the affected component.	5.3	More Details
CVE-2026-82290	Chainlit through 2.12.0 fails to validate ownership of feedback records in PUT and DELETE endpoints. Authenticated attackers can delete or modify other users' feedback by supplying arbitrary feedback identifiers, corrupting human-rating data used for model evaluation.	5.3	More Details
CVE-2026-37067	Incorrect access control in /vfm-admin/admin-panel/view/save-cvs.php in Veno File Manager Project 4.4.9 allows an unauthenticated attacker to extract all application logs from a desired date forwards via a specially crafted POST request.	5.3	More Details
CVE-2026-13406	The Royal Addons for Elementor WordPress plugin before 1.7.1066 does not perform any capability or nonce check before returning taxonomy term data for an arbitrary, caller-supplied taxonomy, allowing unauthenticated users to disclose the names and IDs of terms belonging to non-public taxonomies.	5.3	More Details
CVE-2026-59315	The Spring Cloud Config Monitor is susceptible to Denial of Service attacks via malicious payloads. Spring Cloud Config 5.0.0 - 5.0.4 Spring Cloud Config 4.3.0 - 4.3.4 Spring Cloud Config 4.0.0 - 4.2.8 Spring Cloud Config 3.1.14 and earlier	5.3	More Details
CVE-2026-81560	A vulnerability was identified in blackms aistack up to 1.6.1. Affected by this issue is some unknown functionality of the file src/web/server.ts of the component Static File Handler. Such manipulation of the argument req.url leads to path traversal. The attack can be executed remotely. The exploit is publicly available and might be used. The project was informed of the problem early through an issue report but has not responded yet.	5.3	More Details
CVE-2026-14550	The WPCafe WordPress plugin before 3.0.18 does not perform an authorization check when creating a reservation through its REST API, verifying only a publicly available nonce, allowing unauthenticated users to submit reservations with an arbitrary approval status and bypass the administrator moderation workflow.	5.3	More Details
CVE-2026-37064	User enumeration in /vfm-admin/ajax/usr-check.php in Veno File Manager Project 4.4.9 allows an unauthenticated attacker to enumerate the application users via sending a specially crafted POST request to the affected endpoint with a chosen 'user_name' parameter to test if the user exists.	5.3	More Details
CVE-2026-82698	A vulnerability was detected in sambitraj Student-Management-System up to 56ba287f2e9031523ccb4244cb6e3fe530e4e5d5. This affects an unknown function of the file aca.sql. Performing a manipulation results in use of default password. Remote exploitation of the attack is possible. The exploit is now public and may be used. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided. The project was informed of the problem early through an issue report but has not responded yet.	5.3	More Details
CVE-2026-82220	Unauthenticated Other Vulnerability Type in Forminator <= 1.57.1 versions.	5.3	More Details
CVE-2026-77507	Weblate is a web-based continuous localization platform used to manage software translations. In versions prior to 2026.8, Weblate's object-scoped RSS feeds do not apply the permission checks used elsewhere, allowing unauthorized users to read change-history metadata from private projects and restricted components. On installations that permit anonymous access, this metadata can be retrieved without any authentication. The exposed information can include project and component identities, contributor usernames and full names, action types, timestamps, and translation or unit links, though translated-string content is not included in the feed. Installations using private projects or restricted components are affected. This issue is fixed in version 2026.8.	5.3	More Details
CVE-2026-47874	The vulnerability occurs when a client sends HTTP/1.1 pipelined requests over a single connection, causing the Reactor Netty HTTP server to consume an excessive amount of memory. Reactor Netty 1.3.0 - 1.3.6 Reactor Netty 1.1.0 - 1.2.18 Reactor Netty 1.0.52 and earlier	5.3	More Details
CVE-2026-77754	The Kirki WordPress plugin before 6.0.14 does not perform a capability check on some endpoints of one of its public AJAX actions, allowing unauthenticated users to retrieve the email addresses of registered users	5.3	More Details

	and comment authors, as well as non-public page content and settings.		
CVE-2026-81276	Unauthenticated Broken Access Control in Kali Forms <= 2.4.23 versions.	5.3	More Details
CVE-2026-82591	A security vulnerability has been detected in Open Asset Import Library Assimp up to 6.0.2. The impacted element is the function MD5Importer::MakeDataUnique of the file code/AssetLib/MD5/MD5Loader.cpp. The manipulation of the argument iNewIndex leads to heap-based buffer overflow. The attack can only be performed from a local environment. The identifier of the patch is bf9dabb617c46e5133dac65cca6bff177917afcb. Applying a patch is the recommended action to fix this issue.	5.3	More Details
CVE-2026-19094	The Tutor LMS WordPress plugin before 4.0.6 does not validate values used to build a database query, and does not restrict which template file a request may load, allowing unauthenticated users to inject SQL and to read question and answer content belonging to courses that are not publicly available. The injected text reaches the query as grammar rather than as data, and on the database engines tested it does not yield extraction of arbitrary data, so the confidentiality impact is the disclosed course content rather than the database at large.	5.3	More Details
CVE-2026-13404	The Royal Addons for Elementor WordPress plugin before 1.7.1066 does not perform any capability or ownership check (relying only on a publicly-scrapeable nonce) before writing like-count and visitor-tracking post meta keyed on an arbitrary post ID, allowing unauthenticated users to modify that metadata on any post, including private and draft posts.	5.3	More Details
CVE-2026-80207	APITable through 1.13.0-beta.1 annotates the create handler of InternalNotifyController with requiredLogin = false. ResourceInterceptor honours that annotation by returning before any session or API key is validated, and the nginx gateway shipped with the product proxies every /api request to the backend server, so POST /api/v1/internal/notification/create is reachable by any unauthenticated client that can reach the gateway. An attacker can persist arbitrary notifications in apitable_player_notification against any user ID they name, and because fromUserId can be set to 0 the message is stored with the system sender and renders in the victim's inbox as a legitimate system notification. The body extras content is stored verbatim and forwarded to the frontend.	5.3	More Details
CVE-2026-82548	A vulnerability was determined in Linux Foundation Magma 1.9.0. The impacted element is an unknown function of the component InitialUEMessage Handler. This manipulation causes information disclosure. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized.	5.3	More Details
CVE-2026-81777	Authentication Bypass by Spoofing vulnerability in WPDeveloper Essential Addons for Elementor allows Identity Spoofing. This issue affects Essential Addons for Elementor: from n/a through 6.8.0.	5.3	More Details
CVE-2026-12514	The Shared Files WordPress plugin before 1.7.67, shared-files-pro WordPress plugin before 1.7.70 do not perform a capability check in their file-upload handler, which is registered for unauthenticated users and protected only by a nonce that is output on public pages, so an unauthenticated visitor can upload files to a publicly accessible directory and read the server's absolute path from the response. Uploads are limited to WordPress's allowed MIME types, so executable PHP cannot be uploaded.	5.3	More Details
CVE-2026-82803	A vulnerability has been found in armink struct2json 1.0. This affects the function S2J_STRUCT_GET_string_ELEMENT in the library struct2json/inc/s2jdef.h of the component JSON Deserialization. The manipulation of the argument valuestring leads to null pointer dereference. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2026-70449	Improper validation of resource URL attributes in Apache Wicket allows an unauthenticated remote attacker to read files from the web application, including files under WEB-INF that the servlet container would not otherwise serve. The locale, style and variation attributes decoded from a package resource URL are spliced into the resource lookup path without being checked for path separators. The IPackageResourceGuard — whose rejection of .. is one of the two intended controls — is applied to the resource name before those attributes are appended, and WebApplicationPath rejects only paths literally beginning with WEB-INF/. Neither control ever inspects the attacker-controlled portion of the path. On servlet containers that normalize .. in ServletContext.getResource(), a crafted request therefore escapes the intended package directory. The set of readable files is limited to the file extensions permitted by the configured IPackageResourceGuard. The default SecurePackageResourceGuard permits only js, css, png, jpg, jpeg, gif, ico, cur, map, html, txt, swf, bmp, svg, avif, eot, ttf, woff and woff2, which excludes configuration formats. Applications that have added patterns to the guard, or replaced it with the blocklist-based PackageResourceGuard, can additionally disclose configuration files such as web.xml. Independently of the extension, the lookup performed before the guard runs acts as an existence oracle for arbitrary paths. This issue affects Apache Wicket 8.18.0 and before, 9.23.0 and before and 10.10.0 and before. Users are recommended to upgrade to version 8.19.0, 9.24.0 or 10.11.0, which fix the issue. Users of Apache Wicket 7.x or older, which are no longer supported, should upgrade to a supported version.	5.3	More Details
CVE-2026-77013	The 爱采集数据采集和发布插件 WordPress plugin through 1.0.0 does not restrict which of its handler methods a request may invoke, and performs no capability or nonce check on them, allowing unauthenticated users to create WordPress user accounts and taxonomy terms.	5.3	More Details

CVE-2026-82623	A vulnerability was detected in open62541 up to 1.5.5. Affected by this vulnerability is the function UA_DataValue_backend_copyRange of the file plugins/historydata/ua_history_data_backend_memory.c of the component History Backend. The manipulation results in use after free. The attack can be launched remotely. The exploit is now public and may be used. The project closed the issue report, stating that this is not the official way to report a security vulnerability.	5.3	More Details
CVE-2026-82637	browser-use web-ui versions 2.0.0 through 3.0.0 fail to validate browser settings paths in run_agent_task, allowing attackers to create directories at arbitrary locations by supplying absolute paths to save_recording_path, save_trace_path, save_agent_history_path, or save_download_path parameters. Attackers can exploit this via the unauthenticated Gradio interface to create directories anywhere the root-running container has write access.	5.3	More Details
CVE-2026-82624	A flaw has been found in code-projects Simple Inventory System 1.0. Affected by this issue is some unknown functionality of the file inventorymanagement.sql of the component Database Backup File Handler. This manipulation causes information disclosure. The attack may be initiated remotely. The exploit has been published and may be used.	5.3	More Details
CVE-2026-19430	The Catfolders Document Gallery Pro WordPress plugin before 2.0.7 does not authorise some of its REST API routes, and the token identifying the requested content is forgeable client side, allowing unauthenticated users to list and download the contents of folders that were never published on the site.	5.3	More Details
CVE-2026-3235	The WP Data Access plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 5.5.68 via the 'check_app_access' function due to missing validation on a user controlled key. This makes it possible for unauthenticated attackers to access data from protected app containers by exploiting a mismatch between the authorization check (performed against app_id) and data retrieval (performed using cnt_id without verifying container ownership).	5.3	More Details
CVE-2026-16986	The Booking Package WordPress plugin before 1.7.25 does not validate the payment amount server-side against the stored service price, deriving the expected charge from attacker-supplied request values instead, so an unauthenticated attacker can pay an arbitrary fraction of a service's real price.	5.3	More Details
CVE-2026-11754	Observable discrepancy vulnerability in Seres Software syWEB allows Account Footprinting. This issue affects syWEB: through 27082026. NOTE: The vendor was contacted and it was learned that the product is not supported.	5.3	More Details
CVE-2026-79483	FastGPT Community Edition 4.10.0 through 4.14.0 are vulnerable to a NoSQL injection in the POST /api/core/chat/getHistories endpoint. An unauthenticated attacker can inject malicious NoSQL operators via crafted JSON payloads to bypass authorization checks, resulting in unauthorized access to chat history titles of all users across the platform.	5.3	More Details
CVE-2024-58379	nodemailer before 6.9.9 contains a regular expression denial of service vulnerability in email parsing when attachDataUrls parameter is set or processing embedded file attachments. Attackers can send specially crafted emails with malicious data URLs or embedded attachments to cause the event loop to hang and deny service.	5.3	More Details
CVE-2026-82476	Memos through 0.30.0 omits the 100.64.0.0/10 carrier-grade NAT address range from SSRF protection in its link-metadata fetcher, allowing unauthenticated attackers to bypass IP validation. Attackers can make the server request internal hosts in that range including cloud metadata services and read page titles and descriptions back.	5.3	More Details
CVE-2026-82669	A vulnerability was detected in klaussilveira GitList 2.0.0. Affected by this issue is the function SimpleXMLElement of the file src/SCM/System/Git/CommandLine.php of the component XML Parsing. Performing a manipulation results in denial of service. The attack is possible to be carried out remotely. The exploit is now public and may be used. Upgrading to version 3.0.0-beta can resolve this issue. The patch is named f67609d52c1812fa8a7ed80eae5e795cfd72115f. It is advisable to upgrade the affected component.	5.3	More Details
CVE-2026-82551	A weakness has been identified in Linux Foundation Magma 1.9.0. Affected is an unknown function of the file ngap_amf_handlers.c of the component NGSetup Handler. Executing a manipulation can lead to state issue. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks.	5.3	More Details
CVE-2026-38819	Multiple memory leaks in openNDS before 11.0.0 allow an unauthenticated attacker on the captive portal network to exhaust all available memory on the device within minutes.	5.3	More Details
CVE-2026-82550	A security flaw has been discovered in Linux Foundation Magma 1.9.0. This impacts an unknown function of the component NGSetupRequest Handler. Performing a manipulation of the argument NG-IoT-DefaultPagingDRX results in improper input validation. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	5.3	More Details
CVE-2026-81724	NLTK before 3.10.3 contains an uncontrolled recursion vulnerability in nltk.featstruct.FeatStructReader that allows unauthenticated attackers to cause a denial of service by supplying deeply nested feature-structure input. Attackers can craft trivial payloads with nested brackets that exceed Python's recursion limit and raise an unhandled RecursionError, crashing applications that parse user-supplied feature structures or feature grammars.	5.3	More Details

CVE-2026-80234	CAYIN CMS-WS and CMS-SE developed by CAYIN Technology have a Missing Authentication vulnerability. Unauthenticated remote attackers can obtain media file lists via specific functionality, resulting in partial information disclosure.	5.3	More Details
CVE-2026-40465	NSP is vulnerable to an open redirect due to insufficient server-side validation of the URL (or redirect) parameter.	5.3	More Details
CVE-2026-47844	In specific scenarios, the Reactor Netty HTTP Server may leak exception details across unrelated requests. In order for this to happen, the server must be configured with Brave Tracing. Reactor Netty 1.3.0 - 1.3.6 Reactor Netty 1.1.0 - 1.2.18 Reactor Netty 1.0.52 and earlier	5.3	More Details
CVE-2026-54084	Wazuh is an open-source security platform providing unified XDR and SIEM protection for endpoints and cloud workloads. In versions 4.0.0 through 4.14.6, a malicious or man-in-the-middle enrollment manager can crash a Wazuh agent during enrollment by returning a malformed key response with fewer than four fields, causing a NULL pointer dereference. The w_enrollment_process_agent_key() routine splits the manager-provided key into four space-separated fields but does not verify that all fields are present before passing them to validators. Because OS_StrBreak() leaves missing trailing entries as NULL and OS_IsValidName() calls strlen() on its argument without a NULL check, a response such as OSSEC K:'1' reaches OS_IsValidName(NULL) and terminates the agent process. Since Wazuh permits enrollment against an unverified manager when no CA certificate is configured, an attacker operating a rogue manager or intercepting the enrollment flow can deterministically crash agents, resulting in denial of service. This issue is fixed in version 4.14.7.	5.3	More Details
CVE-2026-82417	### Summary `qs.stringify` throws a `TypeError` when it serializes an object whose own `constructor` property has a truthy, non-callable `isBuffer` member. `utils.isBuffer` duck-types buffers by calling `obj.constructor.isBuffer(obj)` after checking only that the property is truthy, so a value such as `{ constructor: { isBuffer: "x" } }` makes the call throw `TypeError: obj.constructor.isBuffer is not a function`. ### Details `lib/stringify.js:127` calls `utils.isBuffer` on every non-primitive value it serializes. `utils.isBuffer` (`lib/utils.js:332`) reads `obj.constructor.isBuffer` and invokes it without verifying that it is a function. `constructor` and `isBuffer` are ordinary property names, so any object carrying them as own properties reaches the unchecked call. Such an object can be built from untrusted input. `qs.parse("x[constructor][isBuffer]=y", { plainObjects: true })` or `{ allowPrototypes: true }` keeps the `constructor` key as an own property (the default parse options drop it), and `JSON.parse("{\"a\": {\"constructor\":{\"isBuffer\":\"x\"}}}")` produces the same shape with no qs option involved. Express 4 with its default `query parser` setting and body-parser with `extended: true` both call `qs.parse` with `allowPrototypes: true`, so on those stacks `req.query` and `req.body` can carry the shape directly. #### PoC ```js var qs = require("qs"); qs.stringify(qs.parse("x[constructor][isBuffer]=y", { plainObjects: true })); qs.stringify(JSON.parse("{\"a\":{\"constructor\":{\"isBuffer\":\"x\"}}}")); // TypeError: obj.constructor.isBuffer is not a function // at Object.isBuffer (lib/utils.js:332:78) // at stringify (lib/stringify.js:127:45) ``` #### Fix `lib/utils.js`, applied in e83d321 on `main` and released as v6.16.0: ```diff - return !!(obj.constructor && obj.constructor.isBuffer && obj.constructor.isBuffer(obj)); + return !!(obj.constructor && typeof obj.constructor.isBuffer === "function" && obj.constructor.isBuffer(obj)); ``` Real `Buffer`, `safer-buffer`, and browserify `buffer` polyfill instances serialize exactly as before; only the throw is removed. ### Affected versions `>=2.2.5 <6.16.0`, fixed in v6.16.0. The unguarded duck-type was introduced in 3768a75 and first shipped in v2.2.5 (September 2014). v2.2.4 and earlier used `Buffer.isBuffer` and are not affected. Every release from v2.2.5 through v6.15.3 contains the unguarded call. ### Impact An unauthenticated request can make any code path that re-serializes attacker-influenced data with `qs.stringify` (for example, rebuilding a query string from `req.query` for a redirect or an upstream request, or serializing a parsed JSON body) throw synchronously. In a typical Node.js HTTP framework the throw is caught by the framework error boundary and the affected request returns a 500; the process survives and other requests are unaffected. Where the call runs outside an error boundary, such as an `async` Express 4 handler (where the throw becomes an unhandled promise rejection) or a background job, the process exits, so the impact in that case depends on the application error handling rather than on qs.	5.3	More Details
CVE-2026-82802	A flaw has been found in NASA earthdata-search 1.0.0. Affected by this issue is the function OpenSearchGranuleSearchLambda of the file serverless/src/openSearchGranuleSearch/handler.js of the component granules Endpoint. Executing a manipulation of the argument openSearchOsdd can lead to server-side request forgery. The attack can be launched remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2026-82256	SvelteKit before 2.69.1 fails to properly validate remote form function payload sizes, allowing attackers to crash the Node process by sending large payloads. Repeated exploitation causes denial of service by repeatedly crashing the application process.	5.3	More Details
CVE-2026-77758	The Stripe Payment Forms by WP Full Pay WordPress plugin before 8.5.1 does not properly verify that a customer portal session has completed its confirmation step before returning data, allowing unauthenticated users to read another customer's subscription and billing information.	5.3	More Details
CVE-2026-78125	The LearnPress WordPress plugin before 4.0.3 does not perform any authorization check on one of its REST endpoints in all versions up to, and including, 4.0.2, allowing unauthenticated attackers to disclose the payment status of arbitrary orders by enumerating order identifiers.	5.3	More Details
	The Everest Forms plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 3.4.4. This is due to the `load_previous_field_value()` method in `class-evf-form-task.php`		

CVE-2026-5096	accepting arbitrary URL values from `$_POST` data for upload fields without domain restriction, which are then passed to `wp_remote_head()` in the `get_local_file_size()` method of `class-evf-form-fields-upload.php`. This makes it possible for unauthenticated attackers to force the WordPress server to make outbound HTTP HEAD requests to arbitrary URLs by submitting a form with an upload field containing a malicious URL while leaving a required field empty to trigger form re-rendering.	5.3	More Details
CVE-2026-51737	Incorrect access control in the clearTracerouteLog function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to erase traceroute logs via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	5.3	More Details
CVE-2026-14567	The User Frontend WordPress plugin before 4.3.10 does not restrict access to its user directory search endpoint, allowing unauthenticated attackers to retrieve the email address and phone number of every registered user, including administrators.	5.3	More Details
CVE-2026-79706	The Breeze Cache WordPress plugin before 2.5.13 does not sanitise a value taken from the request before using it to build the paths of the files it caches, allowing unauthenticated attackers to create files at arbitrary locations on the server, outside the intended cache directory.	5.3	More Details
CVE-2026-16567	The Document Embedder WordPress plugin before 2.3.1 does not check a document's status before issuing a download token and streaming the file, allowing unauthenticated attackers to download arbitrary Document Embedder WordPress plugin before 2.3.1 documents, including private and draft ones, by enumerating IDs.	5.3	More Details
CVE-2026-77701	The WCFM Marketplace WordPress plugin before 3.8.2 does not correctly verify that the person requesting a refund owns the order, allowing unauthenticated users to create refund requests against any guest checkout order on the site.	5.3	More Details
CVE-2026-81033	Automatisch reveals whether an address is registered through the response to its forgot-password request. The controller at packages/backend/src/controllers/internal/api/v1/users/forgot-password.js looks the address up and chains a not-found throw onto the query, so an address with no account raises an error that the global handler renders as a not-found status, while a registered address proceeds to send the reset message and returns no-content. The route is mounted without authentication. Submitting candidate addresses and comparing the two status codes therefore establishes which addresses hold accounts, with no credential and no rate limiting in the path.	5.3	More Details
CVE-2026-15603	morgan is an HTTP request logger middleware for Node.js. In versions prior to 1.12.0, the internal helper that escapes log token values did not neutralize the Unicode line separator characters U+0085 (Next Line), U+2028 (Line Separator), and U+2029 (Paragraph Separator). An unauthenticated remote client can place these characters in an attacker-controlled log token, for example a Basic auth username surfaced through the remote-user token, so that Unicode-aware downstream log processing splits a single request log into multiple logical records. This is a log forging issue (CWE-117) and an incomplete-fix follow-up to CVE-2026-5078, which only addressed ASCII control characters. The issue is fixed in morgan 1.12.0, which extends the escaping set to cover these Unicode line separators. Upgrade to morgan 1.12.0 to remediate.	5.3	More Details
CVE-2026-74010	Missing Authorization vulnerability in John James Jacoby bbPress allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects bbPress: from n/a through 2.6.14.	5.3	More Details
CVE-2026-82449	Cockpit CMS before 2.14.1 contains an account enumeration vulnerability in the auth check endpoint due to timing discrepancies in password verification. Attackers can measure response times across multiple requests to determine which accounts exist by observing that existing accounts trigger bcrypt verification while non-existent accounts return immediately.	5.3	More Details
CVE-2026-82248	gix-worktree-state before 0.33.0 (part of gitoxide) allows writing files outside the worktree on Windows. gix_worktree_state::checkout() follows an existing terminal symlink during non-exclusive (incremental) materialization (destination_is_initially_empty: false) when core.symlinks is true. If a symlink entry (mode 120000) is first checked out at a path P pointing outside the worktree, a subsequent incremental checkout of a regular-file entry (mode 100644) at the same path follows the existing reparse point and writes the blob content through the link, overwriting files outside the worktree.	5.3	More Details
CVE-2026-51732	Incorrect access control in the delWiFiScheduleCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to remove Wi-Fi schedule entries via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	5.3	More Details
CVE-2026-77184	In MongoDB Connector for BI, the description text of a collection's JSON schema validator is incorporated into the comment text of the DDL returned by SHOW CREATE statements without complete escaping of backslash characters. A user with permission to modify a collection's schema validator, in deployments configured to build their SQL schema from those validators, can cause additional SQL text to be embedded in that generated output. If an operator or automated tool later replays that generated statement against a SQL server, the additional text is executed with the privileges of that session.	5.2	More Details
CVE-2026-81716	openssl_encrypt (pip: openssl-encrypt) versions before 1.4.9 contain a path traversal flaw in PluginSandbox._is_safe_path, which authorized file access using a bare string-prefix match. A sandboxed plugin without the READ_FILES permission could read or write another plugin's directory that merely shares a name prefix (e.g., .../plugins/foobar matching allowed .../plugins/foo), breaking per-plugin isolation within	5.2	More Details

	the same user. Fixed by matching each allowed directory exactly or with a trailing path separator.		
CVE-2026-55425	Graylog is a free and open log management platform. From 7.1.0 until 7.1.4 and 7.2.0-alpha.2, the System Catalog entity titles endpoint in graylog2-server/src/main/java/org/graylog2/rest/resources/system/contentpacks/titles/EntityTitleServiceImpl.java allows an authenticated user to request composite display fields without verifying that every selected field is readable. A user can retrieve protected values, including the password hash on a readable user record; ordinary users are limited to their own permitted records, while administrators can retrieve hashes for all users. This issue is fixed in versions 7.1.4 and 7.2.0-alpha.2.	5.0	More Details
CVE-2026-79720	Reflected XSS in Netron versions <=9.1.2 on desktop application through unsanitized node names allows an attacker to hide certain nodes, perform port scanning or abuse a Chrome n-day to achieve Remote Code Execution.	5.0	More Details
CVE-2026-82873	ToolJet through 3.0.0-ee-beta.2 contains authorization bypass vulnerabilities in the POST /api/v2/resources/export endpoint that allow authenticated users to disclose TooljetDB table schemas across workspace boundaries and export app definitions across granular permission boundaries. Attackers can supply a body-provided organization_id parameter to access schemas from other workspaces, or bypass per-app authorization gates to export restricted app definitions within their workspace.	5.0	More Details
CVE-2026-82486	A vulnerability was found in SiteServer SSCMS 7.4.0. Affected by this issue is some unknown functionality of the component Agent Installation Workflow. Performing a manipulation of the argument SecurityKey results in improper access controls. Remote exploitation of the attack is possible. The attack is considered to have high complexity. The exploitation is known to be difficult. The project was informed of the problem early through an issue report but has not responded yet.	5.0	More Details
CVE-2026-82594	A vulnerability has been found in LogNet grpc-spring-boot-starter up to 5.2.0. Affected is an unknown function of the component Annotation Processing. Such manipulation leads to improper authorization. The attack may be performed from remote. A high complexity level is associated with this attack. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	5.0	More Details
CVE-2026-55067	Vikunja is an open-source self-hosted task management platform. Prior to 2.4.0, POST /api/v1/projects/{project}/views/{view}/buckets/{bucket} allows the request body project_view_id value to be mass assigned by Bucket.Update in pkg/models/kanban.go. The permission check validates that the bucket currently belongs to the URL project and view but does not validate the body selected destination view, allowing any authenticated user to relocate an attacker-owned bucket into another tenant’s Kanban view. The injected bucket retains attacker-controlled content and ownership, enabling cross-tenant defacement. This issue is fixed in version 2.4.0.	5.0	More Details
CVE-2026-18374	Passing an effectively empty string to the `,ccs=` syntax extension of the mode argument in the `fopen` function in the GNU C Library version 2.45 or earlier may result in a heap buffer overflow when the mode string input to the function is attacker controlled. This usage pattern is not seen in applications in common GNU/Linux distributions and applications that process user-supplied values for `ccs` should not pass them through without validation.	4.9	More Details
CVE-2026-82853	Nodemailer versions before 8.0.5 contain an SMTP command injection vulnerability in the transport name option used in EHLO/HELO commands. The name parameter is concatenated directly into SMTP commands without sanitizing carriage return and line feed characters, allowing attackers to inject arbitrary SMTP commands for email spoofing and phishing attacks.	4.9	More Details
CVE-2026-81272	Editor Broken Access Control in FluentPlayer Pro <= 1.3.2 versions.	4.9	More Details
CVE-2026-75126	PLANET GS-4210-16P2S V3 firmware before 3.441b260626 contains multiple authenticated stack buffer overflow vulnerabilities in /cgi-bin/dispatcher.cgi. The following handlers copy attacker-controlled POST parameters into fixed-size stack buffers without length validation: web_vlan_membership_edit_dialog_post; web_dai_vlan_post; web_poe_alive_rmtip_post; web_sys_sntp_post; web_tool_upgradeManager_post; web_port_countersClr_post; web_rmon_statisticsClr_post; web_cablediag_copper_post; web_aaa_*Authlist* handlers; web_acl_mgmt_Rules_Apply_post; web_acl_mgmt_Rules_Edit_post; web_acl_*AceDel_post handlers; web_acl_*AceAdd/Edit_post handlers; web_acl_bindAdd_post; web_acl_bindEdit_post; web_snmp_v3view_add_post; web_snmp_v3group_add_post; web_snmp_v3community_add_post; web_snmp_v3host_add_post; web_snmp_notifyv3_add_post; web_snmp_v3user_add_post; web_snmpv3_remote_engineId_add_post; web_stp_globalSetting_post; web_isg_db_post; web_tacplus*_post handlers; web_dhcp_option82_post; and web_dhcp_port_option82_cid_post. A remote authenticated attacker can send crafted requests to crash the CGI process or web management service, resulting in denial of service.	4.9	More Details
CVE-2026-77786	The Rank Math SEO WordPress plugin before 1.0.277 does not check that the user requesting an automated SEO fix holds the capability WordPress itself requires for the settings being changed, allowing users with the Editor role to modify site-wide core WordPress settings that are reserved to administrators.	4.9	More Details
	ZLMediaKit confines the downloadFile API to a configured set of root directories with a prefix comparison that does not account for directory boundaries. The configuration loader in server/WebApi.cpp builds each		

CVE-2026-81028	root with File::absolutePath("", item, true); because the relative-path argument is empty that helper returns the value without a trailing separator. The handler then accepts a requested path when start_with(file_path, root) holds, so a sibling directory whose name merely begins with the configured root string satisfies the test and is served. The only other guard rejects a path containing two dots, which this requires none of. The equivalent confinement check for the ordinary static file server in src/Http/HttpFileManager.cpp computes its root with a non-empty second argument, which appends the separator before comparing, and so is not affected. The endpoint requires the configured API secret, so this grants no privilege beyond what that secret already implies, but it reads files outside the directory the operator confined it to, and the reference container runs the server as root.	4.9	More Details
CVE-2026-75125	PLANET GS-4210-16P2S V3 firmware before 3.441b260626 contains an authenticated null pointer dereference vulnerability in /cgi-bin/dispatcher.cgi. The web_poe_alive_rmtip_post handler dereferences the rmtIP parameter without verifying its presence. A remote authenticated attacker can send a crafted request omitting the rmtIP parameter to cause the CGI process to dereference a null pointer and crash, resulting in denial of service of the web management interface.	4.9	More Details
CVE-2026-47894	Spring Cloud Config Server native environment repository allows exposure of configuration files outside of the configured repository path. Spring Cloud Config 5.0.0 - 5.0.4 Spring Cloud Config 4.3.0 - 4.3.4 Spring Cloud Config 4.0.0 - 4.2.8 Spring Cloud Config 3.1.14 and earlier	4.9	More Details
CVE-2026-77217	PLANET GS-4210-16P2S V3 firmware before 3.441b260626 contains authenticated stack buffer overflow and null pointer dereference vulnerabilities in /cgi-bin/dispatcher.cgi. The web_radiusSrv*_post family of handlers copies the radKey, radKey_0, radDftParamKey, radName, and radIp POST parameters into fixed-size stack buffers without length validation, and additionally dereferences radName and radIp without verifying their presence in the request. A remote authenticated attacker can send crafted requests to crash the CGI process or web management service, resulting in denial of service.	4.9	More Details
CVE-2026-77218	PLANET GS-4210-16P2S V3 firmware before 3.441b260626 contains authenticated stack buffer overflow vulnerabilities in /cgi-bin/dispatcher.cgi. The web_login_first_post handler copies the usrPass POST parameter into a fixed-size stack buffer without length validation, the web_sys_enablePasswd_post handler copies the enbPass POST parameter into a fixed-size stack buffer without length validation, and the web_sys_localUser_post handler copies the usrName and usrPass POST parameters into fixed-size stack buffers without length validation. A remote authenticated attacker can send a crafted request to crash the CGI process or web management service, resulting in denial of service.	4.9	More Details
CVE-2026-82651	SiYuan before v3.8.1 does not apply the IsForbiddenAbsPath guard (introduced in GHSA-c8r8-95hg-mp34) to the /history/*path and /repo/diff/*path endpoints in kernel/server/serve.go. These routes require admin authentication but construct file paths independently, so an authenticated administrator can retrieve historical snapshots of sensitive files that the guard is meant to block, including data/.siyuan/publishAccess.json (plaintext publish-mode passwords) and files under data/templates/.	4.9	More Details
CVE-2026-63179	Winter CMS is a content management system built on the Laravel PHP framework. In versions up to and including 1.2.12, authenticated backend users can disclose arbitrary files readable by the PHP process by injecting @import (inline) directives into LESS source that the backend compiles, because the LESS parser was instantiated without a safe import resolver and fell back to the raw attacker-supplied path when no allowed root matched. The flaw is reachable through four entry points that share the same root cause: the Brand Settings custom_css field, the Editor Settings html_custom_styles field, the Mail Brand Settings colour-picker fields whose values are concatenated into LESS source without escaping, and theme .less, .sass, and .scss assets compiled when served. Both absolute paths and .. traversal outside the asset's own tree were accepted, so an attacker could read any file the web process can access, most significantly the application .env file and the APP_KEY and database credentials it contains. Exploitation requires a backend account holding one of the associated permissions, which are assigned by default to the built-in Developer role. This issue is fixed in version 1.2.13.	4.9	More Details
CVE-2026-39070	WordPress plugin (Bit Assist) before 1.7.2 is affected by Stored Cross-Site Scripting in Call-To-Action feature. An authenticated attacker with the privileged role (admin) can exploit this to redirect user to malicious site or control the account.	4.8	More Details
CVE-2026-47834	Spring Data JPA's Sort validation can be bypassed when parameters containing crafted payload are accepted from untrusted sources. Spring Data JPA 4.1.0 Spring Data JPA 4.0.0 - 4.0.6 Spring Data JPA 3.5.0 - 3.5.13 Spring Data JPA 3.0.0 - 3.4.15	4.8	More Details
CVE-2026-82258	SvelteKit versions from 2.38.0 before 2.60.1 contain a race condition in query.batch that allows concurrent requests from different users to merge under a single request context. Attackers can exploit specific timing conditions to access sensitive data from other users' concurrent requests.	4.8	More Details
CVE-2026-33606	Mail content stored by a user can be crafted so that it is interpreted as dsync protocol commands when an administrator later runs dsync with the stream protocol, for example during a migration. Injected commands can modify mailbox state on the destination during migration or replication, including internal mailbox attributes that a user should not be able to set directly. It can also cause dsync errors. Avoid running dsync with the stream protocol on mailboxes with untrusted content. Update to non-vulnerable version. No publicly available exploits are known.	4.8	More Details
	The Newsletters WordPress plugin before 4.17 does not generate its API key using a sufficiently random		

CVE-2026-17520	source, deriving it from a publicly known value, allowing unauthenticated attackers to compute the key and perform privileged actions such as adding and deleting subscribers and sending emails, when the optional API has been enabled.	4.8	More Details
CVE-2026-13414	The CMP WordPress plugin before 4.1.18 does not perform authorization checks on one of its AJAX actions and relies on a nonce that is skipped for certain (and exposed to anonymous visitors on others), allowing unauthenticated attackers to disable the site's maintenance/coming-soon mode under a non-default countdown configuration.	4.8	More Details
CVE-2026-81026	The MasterStudy LMS WordPress Plugin WordPress plugin before 3.7.40 does not verify the amount, receiver, currency or status of a payment notification before marking the corresponding order completed, allowing unauthenticated users to complete full-price orders and gain access to paid content by paying only a token amount.	4.8	More Details
CVE-2026-14212	The Booking for Appointments and Events Calendar WordPress plugin before 9.8 does not verify that an authenticated employee (provider) owns the provider account being updated, allowing any employee with an Employee Panel login to overwrite another employee's cabinet password and take over their account.	4.7	More Details
CVE-2026-80200	Kimai before 2.53.0 contains an open redirect vulnerability in the SAML authentication success handler that accepts unvalidated RelayState POST parameters as redirect destinations. Attackers with IdP access can supply malicious RelayState values to redirect authenticated users to attacker-controlled URLs for credential theft or phishing attacks.	4.7	More Details
CVE-2026-81342	The MasterStudy LMS WordPress Plugin WordPress plugin before 3.7.43 does not validate a redirect parameter supplied during user registration before using it, allowing unauthenticated attackers to redirect users to arbitrary external URLs.	4.7	More Details
CVE-2026-82678	A vulnerability was identified in diem-project diem up to 5.1.3. The affected element is the function executeCommand of the file dmAdminPlugin/modules/dmConsole/actions/actions.class.php of the component Administrative Console. Such manipulation of the argument dm_command leads to os command injection. The attack can be launched remotely. The exploit is publicly available and might be used. The project was informed of the problem early through an issue report but has not responded yet.	4.7	More Details
CVE-2026-82468	Rodauth before 2.47.0 contains a cross-site request forgery protection bypass vulnerability in the JSON request content type validation. Attackers can craft cross-origin form posts with content types containing application/json substrings to bypass CSRF token validation and force victims to authenticate to attacker-controlled accounts.	4.7	More Details
CVE-2026-82667	A vulnerability has been found in yaojingang GEOFlow up to 2.1.0. Impacted is the function DistributionController.isValidHttpEndpoint of the file app/Services/GeoFlow/GenericHttpEndpointResolver.php. Such manipulation of the argument endpoint_url leads to server-side request forgery. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 2.1.1 is recommended to address this issue. The name of the patch is 67abfd864a15d169a78429f3290c91cb3b93e849. It is advisable to upgrade the affected component.	4.7	More Details
CVE-2026-82274	Twenty through 2.35.0 contains an open redirect vulnerability in the OAuthPropagatorController.propagateOAuthCallback endpoint that treats the state query parameter as a redirect URL. Attackers can craft malicious requests to redirect users to arbitrary hosts while forwarding OAuth authorization codes, bypassing domain validation when IS_MULTIWORKSPACE_ENABLED is disabled.	4.7	More Details
CVE-2026-81893	A flaw was found in gdk-pixbuf. When loading a specially crafted JPEG image containing chunked ICC profile markers, an error during ICC profile parsing can leave stale size metadata after the profile buffer is freed. A subsequent allocation in the same decode can cause an out-of-bounds write, potentially crashing the application. To exploit this flaw, an application using gdk-pixbuf must process the malicious JPEG image. Affected version >= 2.26.4	4.7	More Details
CVE-2026-82666	A flaw has been found in yaojingang GEOFlow up to 2.1.0. This issue affects the function preview of the file app/Http/Controllers/Admin/SiteThemeEditorController.php of the component Superadmin Theme Editor. This manipulation of the argument blade causes code injection. It is possible to initiate the attack remotely. The exploit has been published and may be used. Upgrading to version 2.1.1 is capable of addressing this issue. Patch name: 67abfd864a15d169a78429f3290c91cb3b93e849. Upgrading the affected component is advised.	4.7	More Details
CVE-2026-82467	Rodauth before 2.47.0 fails to validate protocol-relative return-to paths in confirm_password, login_return_to_requested_location, and two_factor_auth_return_to_requested_location features. Attackers can craft paths with leading double slashes that browsers resolve as protocol-relative URLs, redirecting authenticated users to attacker-controlled sites after login or password confirmation.	4.7	More Details
CVE-2026-82629	A vulnerability was determined in jeecgboot jeewx-boot up to 641ab52c3e1845fec39996d7794c33fb40dad1dd. This issue affects the function MyJwWebJwid3Controller.doUpload of the file jeewx-boot-module-weixin/src/main/java/com/jeecg/p3/open/web/back/MyJwWebJwid3Controller.java of the component doUpload Endpoint. Executing a manipulation of the argument File can lead to unrestricted upload. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized. This product implements a	4.7	More Details

	rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable. The project was informed of the problem early through an issue report but has not responded yet.		
CVE-2026-81681	openssl_encrypt (pip package openssl-encrypt) versions <= 1.4.8 advertise a portable USB workspace as an 'Encrypted USB Workspace' with AES-256-GCM encryption and write a marker declaring the workspace encrypted, but the workspace directory is actually stored in cleartext and the derived encryption key is never applied to it. A user who trusts the branding and places files in the workspace leaves them unencrypted on the removable media, so an attacker with physical access to the media can read the sensitive files. Fixed in 1.4.9, which seals the workspace into an authenticated AES-256-GCM vault.	4.6	More Details
CVE-2026-71378	ResourceIsolationRequestCycleListener protects a Wicket application against cross-site request forgery by rejecting requests that a resource isolation policy judges to come from another origin. Its default policy, FetchMetadataResourceIsolationPolicy, was derived from a reference implementation written to guard static resources, and it inherited two allowances that are unsafe when the thing being guarded is an action on a page: * Every "simple top-level navigation" was allowed. Any GET request carrying Sec-Fetch-Mode: navigate whose Sec-Fetch-Dest was neither object nor embed was allowed, whatever Sec-Fetch-Site said — including cross-site. Wicket invokes component listeners (Link.onClick(), form submits, behaviour callbacks) through ordinary GET navigations, so a page under an attacker's control could navigate the victim's browser to a listener URL and have that listener run inside the victim's authenticated session. Browsers send SameSite=Lax cookies — the effective default when no SameSite attribute is set — on cross-site top-level GET navigations, so the victim's session cookie accompanied the request. * Sec-Fetch-Site: same-site was allowed unconditionally. That value means the same registrable domain and scheme but a different origin — another subdomain or another port. Any sibling origin could therefore invoke any listener by any method, POST form submits included, and cookies are always sent on same-site requests regardless of SameSite. A hostile sibling origin obtained through a subdomain takeover, through delegated user content, or through an XSS elsewhere on the site could act as the authenticated user. Users are recommended to upgrade to version 9.24.0 or 10.11.0, which fix the issue. Affected versions * Apache Wicket 9.1.0 through 9.23.0 * Apache Wicket 10.0.0 through 10.10.0 Not affected Any release older than 9.1.0: * Apache Wicket 8.x (8.0.0 through 8.17.0). The resource isolation classes do not exist in the 8.x line, which offers only the Origin/Referer-based CsrfPreventionRequestCycleListener. No 8.x release requires a fix. * Apache Wicket 9.0.0. ResourceIsolationRequestCycleListener and FetchMetadataResourceIsolationPolicy were introduced by WICKET-6786 and first shipped in 9.1.0 (released 2020-10-07).	4.6	More Details
CVE-2026-75331	tamguo 1.5.3 is vulnerable to Unrestricted File Upload Leading to Stored XSS. The /uploadFile and /imgUpload endpoints in FileUploadController.java and UEditorController.java have no file type validation. Attackers can upload arbitrary HTML/JavaScript files to the server.	4.6	More Details
CVE-2026-73839	Administrative credentials may be exposed in plaintext within the Ebyte device's management interface, increasing the risk of credential compromise through visual or remote observation. This undermines the confidentiality of device access.	4.6	More Details
CVE-2026-76794	MongoSQL Transition Readiness Tool does not sufficiently encode database metadata before including it in generated HTML. A MongoDB user with write access can introduce crafted metadata that may cause script code to run when another user generates and opens the report, potentially exposing report contents or altering its display.	4.6	More Details
CVE-2026-54179	backpack/crud provides Create, Read, Update & Delete (CRUD) functions for Backpack, a collection of Laravel packages that help users build custom administration panels. From 6.0.0 until 6.8.14 and 7.0.37, the src/app/Library/Uploaders/SingleBase64Image.php methods SingleBase64Image::uploadFiles and SingleBase64Image::uploadRepeatableFiles, used by image fields through withFiles(), accept any data URI beginning with data:image without validating the declared MIME subtype or decoded bytes, while src/app/Library/Uploaders/Support/FileNameGenerator.php method FileNameGenerator::getExtensionFromFile applies mime_content_type() to the data URI instead of the decoded content. An authenticated administrator can therefore store arbitrary file content under an extensionless filename on the configured disk, which can cause stored cross-site scripting or other unintended behavior when the file is served and accessed. This issue is fixed in version 7.0.38 and 6.8.14.	4.4	More Details
CVE-2026-82670	A flaw has been found in IObit Uninstaller 15.5.0.11. This affects the function IRP_MJ_DEVICE_CONTROL in the library IUForceDelete.sys of the component IOCTL Handler. Executing a manipulation can lead to improper privilege management. The attack requires local access. The vendor was contacted early about this disclosure but did not respond in any way.	4.4	More Details
CVE-2026-75573	In MongoDB Connector for BI, mongodrdl may write a TLS private-key password to standard error when the password is supplied through both the connection URI and the corresponding command-line option. A local user with access to the captured command output and encrypted key file may use the disclosed password to access the associated TLS client key.	4.4	More Details
CVE-2026-82865	pdfme schemas before 5.5.10 contains a cross-site scripting vulnerability in the multiVariableText property panel that assigns unsanitized i18n label values to innerHTML. Attackers who control label overrides through options.labels can inject arbitrary JavaScript that executes when users open the Designer and select a multiVariableText field without variable placeholders.	4.4	More Details
	A missing input-validation issue in MongoDB libmongocrypt's automatic-encryption context setup allows a		

CVE-2026-81523	caller-supplied database identifier to be accepted without sanitization. The resulting impact is limited to incorrect schema selection, which may lead to limited disclosure or modification of information handled by the application.	4.4	More Details
CVE-2026-61790	Weblate is a web-based continuous localization platform used to manage software translations. In versions prior to 2026.7, a team can require its members to configure two-factor authentication before receiving the team's permissions, but this requirement is not enforced for site-wide global permissions. As a result, a user who belongs to a team that enforces 2FA and grants a global permission still receives that global permission even without 2FA configured, while the same requirement is correctly applied to project-, component-, and workspace-scoped permissions. Such a user can act on the granted global permission, including reaching the site management interface at /manage/. This issue is fixed in version 2026.7.	4.4	More Details
CVE-2026-82650	SiYuan 3.8.0 contains a path traversal / sensitive file exposure vulnerability in the RenderTemplate function (kernel/model/template.go), reachable via the POST /api/template/render endpoint (kernel/api/template.go). The endpoint restricts the supplied path only to the workspace directory (util.IsAbsPathInWorkspace) but, unlike the file API's refuseToAccess() blocklist, applies no sensitive-path exclusion. This allows an authenticated attacker to read sensitive workspace files, including conf/conf.json, which contains the API token and cookie signing key. The issue is fixed in v3.8.1.	4.4	More Details
CVE-2026-21810	HCL BigFix Quantum Risk Analyzer is affected by a hardcoded external resource reference and a lack of binary integrity which could allow an attacker to obtain sensitive information or modify the binary.	4.4	More Details
CVE-2026-58616	Concurrent execution using shared resource with improper synchronization ('race condition') in Copilot Chat (Microsoft Edge) allows an authorized attacker to disclose information over a network.	4.4	More Details
CVE-2026-19454	The JetBackup WordPress plugin before 3.1.23.5 does not perform its multisite authorisation check before serving backup archives and job logs, allowing an administrator of the network's main site who is not a Super Admin to download a full backup of the entire network, including every site's data and the shared webroot.	4.4	More Details
CVE-2026-51656	Incorrect access control in the getVpnPassCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain VPN pass-through and WAN ping filter settings via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	4.3	More Details
CVE-2026-66798	Use after free in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	4.3	More Details
CVE-2026-55064	Vikunja is an open-source self-hosted task management platform. From 2.3.0 until 2.4.0, a user with Write but not Admin permission on a shared child project can detach it from its parent hierarchy by submitting parent_project_id equal to 0 to POST /api/v1/projects/{project}. The Project.CanUpdate authorization check in pkg/models/project_permissions.go and UpdateProject logic in pkg/models/project.go only gate nonzero parent values, while UpdateProject always persists parent_project_id, so the explicit zero value bypasses the Admin requirement introduced for CVE-2026-35595. Detachment severs the recursive permission-inheritance chain and can disrupt the owner’s hierarchy and inherited collaborator access. This issue is fixed in version 2.4.0.	4.3	More Details
CVE-2026-51655	Incorrect access control in the getMacFilterRules function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain MAC filter rules via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	4.3	More Details
CVE-2026-51654	Incorrect access control in the getScheduleCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain schedule or scheduled-reboot configuration information via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	4.3	More Details
CVE-2026-18545	IBM Langflow OSS 1.0.0 through 1.11.1 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 Details
CVE-2026-54614	DebugKit provides a debugging toolbar for CakePHP applications. Prior to 4.10.3 and 5.2.4, the DebugKit MailPreview feature in src/Controller/MailPreviewController.php accepts a route-controlled previewName value in findPreview and passes the resolved class from App::className() to constructor execution without rejecting namespace separators or verifying that the class extends DebugKit\Mailer\MailPreview. An attacker able to access DebugKit while debug mode is enabled and the request hostname is local or allowlisted can select an unintended application class through the mail-preview preview route, resulting in arbitrary constructor execution and limited disclosure of application information. This issue is fixed in versions 4.10.3 and 5.2.4.	4.3	More Details
CVE-2026-82633	Dolibarr versions 10.0.0 before 24.0.0 fail to perform per-object authorization checks in the Users::getGroups REST API endpoint, allowing authenticated users to retrieve group memberships of other users. Attackers can call GET /users/{id}/groups with arbitrary user identifiers to access group names, entity associations, and private notes across tenant boundaries.	4.3	More Details
CVE-2026-	A flaw has been found in wger-project wger up to 2.6.0-alpha2. This issue affects the function reset_user_password of the file wger/gym/views/gym.py of the component Password Reset. Executing a manipulation can lead to cross-site request forgery. It is possible to launch the attack remotely. This patch is	4.3	More

82544	called 3c6ce4b7f3eeafeb35318c6c4e82b1a3fd28b314. It is advisable to implement a patch to correct this issue.		Details
CVE-2026-51652	Incorrect access control in the getUPnPCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain UPnP enablement and parsed port-mapping information via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	4.3	More Details
CVE-2026-55834	Pocket ID is an OIDC provider that allows users to authenticate with their passkeys to services. From 2.6.0 until 2.9.0, frontend/src/routes/authorize/+page.ts reads the redirect_uri query parameter and frontend/src/routes/authorize/+page.svelte uses the raw callbackURL in redirectWithError when prompt=none cannot complete silent authorization. The client-side path only blocks javascript and data schemes and does not invoke the backend callback allow-list validation, so an unauthenticated attacker who knows a valid client_id can redirect a victim browser to an arbitrary HTTP or HTTPS origin for phishing or OIDC error and state smuggling. This issue is fixed in version 2.9.0.	4.3	More Details
CVE-2026-55566	Yamcs is a mission control framework. Prior to 5.12.8 and 5.13.2, Yamcs processes attacker-controlled data from the /ext URL route in yamcs-web/src/main/webapp/projects/webapp/src/app/core/routes/extension.matcher.ts, extension.component.ts, and app.component.ts without checking registered plugin IDs before DOM rendering through innerHTML. A crafted URL can execute JavaScript when opened by a user. The script can read data available to the Yamcs web application and perform actions in the user context. This issue is fixed in versions 5.12.8 and 5.13.2.	4.3	More Details
CVE-2026-55547	Yamcs is a mission control framework. Prior to 5.12.8 and 5.13.2, Yamcs omits SystemPrivilege.ControlAccess checks from IamApi.listRoles, IamApi.getRole, and IamApi.listPrivileges in yamcs-core/src/main/java/org/yamcs/http/api/IamApi.java. Any authenticated account can call GET /api/roles, GET /api/roles/{name}, and GET /api/privileges to enumerate available system privileges and configured role mappings. The disclosure reveals security configuration that can support targeted privilege-escalation attempts. This issue is fixed in versions 5.12.8 and 5.13.2.	4.3	More Details
CVE-2026-80311	The Stripe Payment Forms by WP Full Pay WordPress plugin before 8.5.5 does not verify that a subscription belongs to the customer bound to the requesting customer-portal session before cancelling it, allowing a user with a confirmed portal session to cancel subscriptions belonging to other customers. Exploitation requires the attacker to know the target subscription's identifier, which is high-entropy and not enumerable through the Stripe Payment Forms by WP Full Pay WordPress plugin before 8.5.5.	4.3	More Details
CVE-2026-82111	A vulnerability was detected in iswalle getnote-mcp up to 1.5.0. The affected element is the function fs.readFileSync of the file src/index.ts of the component upload_image. Performing a manipulation of the argument image_path results in path traversal. The attack can be initiated remotely. The exploit is now public and may be used. Upgrading to version 1.5.1 is sufficient to fix this issue. The patch is named 7f9a215e03575c650d38c8f87fc6d8d363fed80d. Upgrading the affected component is advised.	4.3	More Details
CVE-2026-51653	Incorrect access control in the getStorageCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain storage feature state information via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	4.3	More Details
CVE-2026-51635	Incorrect access control in the getWiFiScheduleCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain Wi-Fi scheduling rules via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	4.3	More Details
CVE-2026-51651	Incorrect access control in the getSmartQosCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain Smart QoS configuration and rules via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	4.3	More Details
CVE-2026-55227	Weblate is a web-based localization tool. In versions prior to 2026.7, several endpoints look up objects in a globally scoped manner rather than restricting the lookup to projects the user can access, so they return HTTP 403 (Forbidden) instead of 404 (Not Found) when a user requests an object they are not authorized to see. This difference lets unauthorized users infer whether a given object exists in a private Weblate project. The issue has been fixed in version 2026.7.	4.3	More Details
CVE-2026-81284	Contributor Broken Access Control in ACF Extended <= 0.9.2.6 versions.	4.3	More Details
CVE-2026-81299	Subscriber Insecure Direct Object References (IDOR) in WP Job Portal <= 2.5.9 versions.	4.3	More Details
CVE-2026-71172	Dell Cloud Disaster Recovery, versions 20.2 and prior, contain a Server-Side Request Forgery (SSRF) vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Server-side request forgery.	4.3	More Details
CVE-2026-	Fleet is an open-source device management platform built on osquery. In versions prior to 4.85.0, the global policy read endpoint (GET /api/latest/fleet/policies/{policy_id}) fails to verify team ownership of the requested policy, allowing an authenticated user with observer-level access on any single team to read the full details of policies belonging to any other team and bypass Fleet's team isolation model. The handler authorizes the request against an empty policy object whose TeamID is nil, which an authorization rule	4.3	More

41262	permits for any user holding a role on any team, and then fetches the policy by ID with no team filter and returns it without any post-fetch scope check. Because policy IDs are sequential integers, an attacker can enumerate them to read other teams' policy SQL queries, host pass and fail counts, and associated software-installer and script metadata, exposing security-monitoring strategies and compliance posture across team boundaries. This issue is fixed in version 4.85.0.		Details
CVE-2026-75601	Static Web Server (SWS) is a production-ready web server suitable for static web files or assets. Through 2.43.0, instances with both basic-auth and metrics features enabled process the /metrics endpoint before the basic-auth check in src/handler.rs, allowing an unauthenticated remote attacker to retrieve Prometheus metrics that disclose virtual host names, request volumes, error rates, latency distributions, and active connections. This issue is fixed in version 2.44.0.	4.3	More Details
CVE-2026-47850	Spring Data REST does not preserve the persisted version (@Version) property of an aggregate root when handling an HTTP PUT against an immutable target type. Spring Data REST 5.1.0 Spring Data REST 5.0.0 - 5.0.6 Spring Data REST 4.5.0 - 4.5.12 Spring Data REST 4.0.0 - 4.4.15 Spring Data REST 3.7.20 and earlier	4.3	More Details
CVE-2026-51664	Incorrect access control in the getTelnetCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain Telnet service enablement status information via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	4.3	More Details
CVE-2026-51665	Incorrect access control in the getTracerouteCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain traceroute diagnostic logs via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	4.3	More Details
CVE-2026-51610	Incorrect access control in the RebootSystem function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to arbitrarily force an immediate reboot via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	4.3	More Details
CVE-2026-51614	Incorrect access control in the getAccessDeviceCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain access-device policy and client state information via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	4.3	More Details
CVE-2026-52473	An issue in Wgcloud 3.6.4 allows a remote attacker to escalate privileges via the content parameter is directly concatenated to the ProcessBuilder.	4.3	More Details
CVE-2026-62249	Weblate is a web-based continuous localization platform used to manage software translations. In versions prior to 2026.7, an authenticated user with access to a project can retrieve the change history of restricted components in that project through nested API change endpoints, even without permission to view those components directly. The nested endpoints do not apply the component-level access checks enforced on the direct component views, so the requester can enumerate changes for components that should be hidden from them. The exposed data can include the restricted component's identity, translation and unit links, and change payload fields such as source or translated string content in the target, old, and details values. This issue is fixed in version 2026.7.	4.3	More Details
CVE-2026-51640	Incorrect access control in the getMeshNeighborTable function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain mesh neighbor information via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	4.3	More Details
CVE-2026-55696	PrivateBin is an online pastebin where the server has zero knowledge of pasted data. Prior to 2.0.5, AttachmentViewer.setAttachment in js/privatebin.js uses getAttachmentMimeType to accept attacker-controlled MIME types and uses getBlobUrl to create a same-origin blob before setting attachmentLink's href for the Download attachment link. The SVG-only sanitization branch updates only the preview blob, so text/html, image/svg, application/xhtml+xml, and text/xml attachments can remain active in the download blob. On an instance with fileupload = true and a weakened, stripped, or absent Content Security Policy, an anonymous attacker can create such an attachment, and a victim who opens the link in a new tab causes inline JavaScript to execute in the PrivateBin origin. The script can read origin-scoped local storage and issue same-origin requests, including requests to applications co-hosted on the same domain. This issue is fixed in version 2.0.5.	4.3	More Details
CVE-2026-51629	Incorrect access control in the getStaticDhcpRules function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain static DHCP reservation rules via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	4.3	More Details
CVE-2026-51630	Incorrect access control in the getDdnsCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain DDNS configuration, including domain, username, and password, via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	4.3	More Details
CVE-2026-51631	Incorrect access control in the getStaticDhcpRules function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain WPS runtime status via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	4.3	More Details
CVE-2026-51632	Incorrect access control in the getWiFiAdvancedCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain advanced wireless settings via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	4.3	More Details

CVE-2026-51633	Incorrect access control in the getWiFiEasyGuestCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain simplified guest Wi-Fi configuration, including guest credentials, via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	4.3	More Details
CVE-2026-51634	Incorrect access control in the getWiFiBasicCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain core wireless settings, including SSIDs and Wi-Fi keys, via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	4.3	More Details
CVE-2026-51637	Incorrect access control in the getMeshPortalTable function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain mesh portal table information via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	4.3	More Details
CVE-2026-51638	Incorrect access control in the getWiFiGuestCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain guest Wi-Fi configuration information via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	4.3	More Details
CVE-2026-51639	Incorrect access control in the getApWiFiSchCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain AP-specific Wi-Fi scheduling rules via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	4.3	More Details
CVE-2026-82257	SvelteKit versions before 2.69.1 contain a prototype pollution vulnerability in remote form functions with file input fields that accept arbitrary user-controlled path names. Attackers can manipulate the deletion path to remove methods on the prototype, potentially disabling application functionality.	4.3	More Details
CVE-2026-81761	Subscriber Broken Access Control in WpEvently <= 5.5.0 versions.	4.3	More Details
CVE-2026-51613	Incorrect access control in the getDeviceInfo function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain device identification details via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	4.3	More Details
CVE-2026-82601	A weakness has been identified in SeaCMS up to 13.6. This affects an unknown part of the file /err.php. Executing a manipulation of the argument errtxt can lead to cross site scripting. The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks.	4.3	More Details
CVE-2026-59319	RedisChatMemoryRepository.findByMetadata() builds RediSearch tag and text queries from caller-supplied metadata values without applying RediSearchUtil.escape(), unlike get(), clear(), and findByTimeRange() in the same class which do escape their inputs. An application that passes user-controlled values to findByMetadata() on a tag-typed metadata field allows an attacker to inject RediSearch syntax (e.g. x} | *) that breaks out of the tag clause and matches all indexed chat messages across every conversation in the index. Spring AI 2.0.0	4.3	More Details
CVE-2026-51706	Incorrect access control in the setSmartQosCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to degrade traffic handling via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	4.3	More Details
CVE-2026-79995	The User Registration & Membership WordPress plugin before 5.2.5 does not verify that the account whose pending email change is being cancelled belongs to the user making the request, allowing authenticated users with Subscriber-level access and above to cancel any other user's in-progress email change, including an administrator's.	4.3	More Details
CVE-2026-79654	A flaw was found in Katello where the Content View History API does not properly enforce authorization when accessing a Content View specified by the user. An authenticated user with permission to view Content Views in one organization may be able to access the lifecycle history of a Content View belonging to another organization by supplying its identifier to the affected API endpoint. This can result in unauthorized disclosure of Content View lifecycle information, including publication and promotion events, associated users, and timestamps.	4.3	More Details
CVE-2026-82658	Admidio versions before 5.0.12 contain a broken access control vulnerability in profile_function.php that allows authenticated low-privilege users to read another user's future role memberships. Attackers can bypass profile-level authorization by directly calling the reload_future_memberships endpoint with a victim's user UUID to disclose sensitive membership information.	4.3	More Details
CVE-2026-74930	The Project Manager WordPress plugin before 4.0.7 does not check that the user whose activity is being requested is the one making the request in one of its REST API routes, allowing any authenticated user, such as a subscriber, to read any other user's activity history along with their email address and the details of projects they have no access to.	4.3	More Details
CVE-2026-78138	The Finale Lite WordPress plugin before 2.21.0 does not perform a capability check on an AJAX action that returns a sales-campaign's configuration for an arbitrary post ID, allowing any authenticated user (Subscriber and above) to read the Finale Lite WordPress plugin before 2.21.0's campaign configuration and scheduling data.	4.3	More Details
CVE-2026-	The Notifima WordPress plugin before 3.1.4 does not verify that the caller owns the subscription being modified on one of its REST endpoints in all versions up to, and including, 3.1.3, allowing authenticated		More

78139	attackers with Subscriber-level access to unsubscribe arbitrary customers from product stock-alert notifications.	4.3	Details
CVE-2026-77789	The Stripe Payment Forms by WP Full Pay WordPress plugin before 8.5.1 does not verify that a subscription belongs to the customer bound to the requesting customer-portal session before acting on it, allowing a user with a confirmed portal session to cancel, reactivate or modify subscriptions belonging to other customers.	4.3	More Details
CVE-2026-82554	A flaw has been found in SourceCodester Queue Management System 1.0. This affects an unknown part of the file /api/add_customer.php. This manipulation of the argument Name causes cross site scripting. It is possible to initiate the attack remotely. The exploit has been published and may be used.	4.3	More Details
CVE-2026-51678	Incorrect access control in the setSyslogCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to alter logging behavior via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	4.3	More Details
CVE-2026-50199	Wallos is an open-source, self-hostable personal subscription tracker. Prior to version 4.9.1, endpoints/currency/update_exchange.php loads the first Fixer/API Layer credential globally instead of loading the credential for the authenticated user. As a result, a normal authenticated user without their own provider key can trigger exchange-rate refreshes using another user's stored provider credential. This issue has been patched in version 4.9.1.	4.3	More Details
CVE-2026-50198	Wallos is an open-source, self-hostable personal subscription tracker. Prior to version 4.9.1, an authenticated user can edit their own inactive subscription and set replacement_subscription_id to a subscription ID belonging to another user. The write is accepted, and later the stats logic dereferences that foreign subscription ID without user_id scoping. This lets the attacker infer the victim subscription's monthly-normalized cost by observing changes in their own stats output. This does not expose the full victim subscription object, but it does expose derived financial metadata. This issue has been patched in version 4.9.1.	4.3	More Details
CVE-2026-52730	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 in Module::settingsForm allows to view (not change) super admin-restricted module settings and leak the full module entity. Exploitation of the vulnerability is possible on behalf of an authorized user who has access to the Module View feature, which are not granted to non-admins as standard. Users should upgrade to version 4.4.3 which fixes this issue. Upgrading to a fixed version is necessary to remediate. Users unable to upgrade should revoke such privileges from users they do not trust.	4.3	More Details
CVE-2026-82587	A vulnerability was determined in Open5GS up to 2.7.7. This vulnerability affects the function amf_namf_comm_decode_ue_mm_context_list of the file src/amf/namf-handler.c of the component AMF. This manipulation of the argument ueContext.mmContextList[*].allowedNssai causes memory corruption. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized. Upgrading to version 2.8.0 is able to resolve this issue. Patch name: abf8a836564b966b5141110fc25ed413c4f17522. It is recommended to upgrade the affected component.	4.3	More Details
CVE-2026-15387	GitLab has remediated an issue in GitLab EE affecting all versions from 19.1 before 19.1.7, 19.2 before 19.2.5, and 19.3 before 19.3.1 that, under certain conditions, an authenticated user with developer-role permissions could have influenced the execution environment of Pipeline Execution Policy enforcement jobs, due to improper handling of job dependencies.	4.3	More Details
CVE-2026-82619	A vulnerability was identified in Systerel S2OPC up to 1.7.3. The impacted element is the function monitored_item_event_filter_treatment_bs__init_event_filter_ctx_and_result of the file src/ClientServer/services/bgenc/subscription_mgr.c. Such manipulation of the argument EventFilter leads to use after free. The attack may be performed from remote. The exploit is publicly available and might be used. The name of the patch is a4cee16a851b971be447a6ed531173702c722b99. It is best practice to apply a patch to resolve this issue.	4.3	More Details
CVE-2026-59280	Applications using Spring Framework's FreeMarker integration may be vulnerable to a path traversal attack when a controller returns a view name derived from untrusted input and FreeMarker is configured to resolve templates through SpringTemplateLoader. Spring Framework 7.0.0 - 7.0.8 Spring Framework 6.2.0 - 6.2.19 Spring Framework 6.1.0 - 6.1.28 Spring Framework 6.0.0 - 6.0.30 Spring Framework 5.3.0 - 5.3.49 Spring Framework 5.2.25.RELEASE and earlier	4.3	More Details
CVE-2026-81346	The Frontend Admin by DynamiApps WordPress plugin before 3.29.11 does not perform a capability check on one of its AJAX actions, allowing any authenticated user, such as a subscriber, to delete arbitrary membership plans.	4.3	More Details
CVE-2026-51704	Incorrect access control in the setWiFiMeshConfig function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to alter mesh configurations via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	4.3	More Details
CVE-2026-51702	Incorrect access control in the setIpPortFilterRules function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to alter firewall policies via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	4.3	More Details
CVE-2026-	Improper neutralization of Script-Related HTML tags in a web page (basic XSS) vulnerability in Softtr		More

5218	Informatics Technology Trading Limited Company E-Commerce Pack allows Cross-Site Scripting (XSS). This issue affects E-Commerce Pack: before 5.03.01.49.	4.3	Details
CVE-2026-82588	A vulnerability was identified in Open5GS up to 2.7.7. This issue affects some unknown processing of the file src/amf/namf-handler.c of the component Transfer Endpoint. Such manipulation leads to null pointer dereference. The attack can be launched remotely. Upgrading to version 2.8.0 is capable of addressing this issue. The name of the patch is abf8a836564b966b5141110fc25ed413c4f17522. Upgrading the affected component is advised.	4.3	More Details
CVE-2026-82589	A security flaw has been discovered in Open5GS up to 2.7.7. Impacted is the function amf_namf_comm_handle_n1_n2_message_transfer of the file src/amf/namf-handler.c of the component N1-N2 Message Handler. Performing a manipulation of the argument N1N2MessageTransferReqData.n2InfoContainer.smInfo.n2InfoContent.ngapIeType results in denial of service. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks. Upgrading to version 2.8.0 is recommended to address this issue. The patch is named abf8a836564b966b5141110fc25ed413c4f17522. It is advisable to upgrade the affected component.	4.3	More Details
CVE-2026-82590	A weakness has been identified in Open5GS up to 2.7.7. The affected element is the function smf_nudm_sdm_handle_get of the file src/smf/nudm-handler.c of the component SMF. Executing a manipulation of the argument preemptCap can lead to reachable assertion. The attack may be launched remotely. Upgrading to version 2.8.0 is sufficient to fix this issue. This patch is called 4554405f29bffd7562abedbee63484825bd90cd5. You should upgrade the affected component.	4.3	More Details
CVE-2026-82605	A vulnerability has been found in BareBones BBEdit up to 15.5.5. The affected element is an unknown function of the component Lasso Language Tokenizer. Such manipulation leads to infinite loop. The attack can be executed remotely. Upgrading to version 16.0 is sufficient to fix this issue. The affected component should be upgraded.	4.3	More Details
CVE-2026-82821	A vulnerability was determined in FLVMeta up to 1.2.2. Affected by this vulnerability is the function amf_object_get of the file src/amf.c of the component AMF Object Parsing. This manipulation causes null pointer dereference. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized. Patch name: 52642f7dfb76ec7334016622dde60b1ae963d79b. To fix this issue, it is recommended to deploy a patch. The project maintainer doubts the security impact: "While I acknowledged the bugs and provided fixes, I have yet to see any way to exploit these alleged vulnerabilities."	4.3	More Details
CVE-2026-51683	Incorrect access control in the setLanCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to alter LAN network configuration via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	4.3	More Details
CVE-2026-82820	A vulnerability was found in FLVMeta up to 1.2.2. Affected is the function amf_string_new of the file src/amf.c of the component AMF String Processing. The manipulation of the argument length results in heap-based buffer overflow. The attack can be launched remotely. The exploit has been made public and could be used. The patch is identified as f412a33b9a84c2d1a9dee145a868feddbf64879e. A patch should be applied to remediate this issue. The project maintainer doubts the security impact: "While I acknowledged the bugs and provided fixes, I have yet to see any way to exploit these alleged vulnerabilities."	4.3	More Details
CVE-2026-82700	A vulnerability was found in code-projects Online Shopping System 1.0. Affected by this vulnerability is an unknown functionality of the file /offersmail.php of the component Newsletter Subscription. The manipulation of the argument email results in cross site scripting. The attack may be performed from remote. The exploit has been made public and could be used.	4.3	More Details
CVE-2026-82604	A flaw has been found in BareBones BBEdit up to 15.5.5. Impacted is an unknown function of the component Java Language Module. This manipulation causes uncontrolled recursion. Remote exploitation of the attack is possible. Upgrading to version 16.0 is recommended to address this issue. You should upgrade the affected component.	4.3	More Details
CVE-2026-82618	A vulnerability was determined in Systerel S2OPC up to 1.7.3. The affected element is the function set_range_matrix_on_string_array of the file src/Common/opcua_types/sopc_builtintypes.c of the component String Array Range Writing. This manipulation causes out-of-bounds read. The attack is possible to be carried out remotely. The project was informed of the problem early through an issue report but has not responded yet.	4.3	More Details
CVE-2026-82552	A security vulnerability has been detected in Linux Foundation Magma 1.9.0. Affected by this vulnerability is an unknown functionality of the file tasks/ngap/ngap_amf.c of the component gNB Termination Handler. The manipulation leads to denial of service. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used.	4.3	More Details
CVE-2026-82664	A security vulnerability has been detected in yaojingang GEOFlow up to 2.1.0. This affects an unknown part of the file app/Http/Controllers/Site/HomeController.php of the component JSON-LD Theme Handler. The manipulation of the argument Search leads to cross site scripting. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used. Upgrading to version 2.1.1 is able to mitigate this issue. The identifier of the patch is 67abfd864a15d169a78429f3290c91cb3b93e849. Upgrading the affected component is recommended.	4.3	More Details

CVE-2026-33263	When mail_max_userip_connections is set (default 10) and reached, submission-login can crash with epoll() panic caused by file descriptor handling issues. If running in high-security mode (default for community releases), only the new submission connection gets terminated. If running in high-performance mode (default for Pro releases), all connections handled by the submission-login process will be terminated. The crashes can cause failure for user to send a message, or it can cause duplicate messages to be sent. If TLS is not used (in the backend server processing the submission), duplicate deliveries cannot happen, because the crash can only happen at AUTH stage. Limit the number of connections handled by single submission-login process. This has a performance impact though. Update to non-vulnerable version. No publicly available exploits are known.	4.3	More Details
CVE-2026-82805	A vulnerability was found in Typora up to 1.13.8/1.14.6. This vulnerability affects unknown code of the component Mermaid Rendering Engine. The manipulation of the argument classDef/style results in cross site scripting. The attack may be launched remotely. The exploit has been made public and could be used. Upgrading to version 1.14.8 is able to resolve this issue. You should upgrade the affected component. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.	4.3	More Details
CVE-2026-42395	A host listed as a trusted proxy can send forwarding information containing a NUL byte, which crashes the login process on the following login attempt. The login process is terminated, which can cause degradation or denial of service for logins. Deployments that do not configure trusted proxies are not affected. Restrict the list of trusted proxy networks to hosts that are fully under your control. Update to non-vulnerable version. No publicly available exploits are known.	4.3	More Details
CVE-2026-42392	An attacker that has valid credentials can send an invalid IMAP URLFETCH command, which causes uninitialized memory to be included in the error response returned to the client. Process memory contents can be disclosed to the client, which may include sensitive data. Disable the IMAP URLAUTH functionality. Update to non-vulnerable version. No publicly available exploits are known.	4.3	More Details
CVE-2026-42008	Forwarding information received from a host listed as a trusted proxy is not kept separate from Dovecot's own authentication fields, so a value sent by that host can be injected as an internal authentication field. Any host permitted to act as a trusted proxy can authenticate as any user without knowing that user's password. This affects deployments whose password database honours a field that permits authentication without a password. Deployments that do not configure trusted proxies are not affected. Restrict the list of trusted proxy networks to hosts that are fully under your control. Update to non-vulnerable version. No publicly available exploits are known.	4.3	More Details
CVE-2026-40015	An attacker that has valid credentials can open many connections to the imap-hibernate service and send invalid commands, which can intermittently cause an out-of-bounds read and crash the process. The crash interrupts hibernated IMAP sessions handled by the affected process, which can cause degradation of service for IMAP. Disable IMAP hibernation. Update to non-vulnerable version. No publicly available exploits are known.	4.3	More Details
CVE-2026-40013	An attacker that has valid credentials can submit a Sieve script containing an extreme numeric literal, which causes an out-of-bounds write when the ManageSieve service compiles the script. This causes memory corruption and an observed crash of the ManageSieve process, resulting in denial of service for script management. This might be able to be used for remote code execution. Disable the ManageSieve service if users do not need remote Sieve script management. Update to non-vulnerable version. No publicly available exploits are known.	4.3	More Details
CVE-2026-51666	Incorrect access control in the setWizardCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to reconfigure WAN, Wi-Fi, and device initialization state via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	4.3	More Details
CVE-2026-51667	Incorrect access control in the getWiFiIpMacTable function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to obtain Wi-Fi client MAC-to-IP mappings via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	4.3	More Details
CVE-2026-80194	Kimai before 2.64.0 contains a missing authorization vulnerability in the ProjectViewController export route (report_project_view_export). The authorization guards are attached to the sibling __invoke method rather than at the class level, so the export route inherits no authorization checks. Any authenticated user, including a plain ROLE_USER without the project_reporting permission, can download the project overview export - which returns the same dataset as the protected report - disclosing customer names, project names, currency, budget type, and aggregate totals across all customers. Actual financial figures remain protected in the export template.	4.3	More Details
CVE-2026-33607	An attacker that has valid credentials can use IMAP LIST command to consume CPU. This can cause degradation or denial of service for IMAP. Monitor system for abnormal CPU usage and kill the offending process and lock account. Alternatively install fixed version. No publicly available exploits are known.	4.3	More Details
CVE-2026-16568	The Mobile App for WooCommerce: ShopApper Mobile App Builder Service for WooCommerce WordPress plugin through 0.4.62 does not verify that the requesting user owns the customer profile being queried through one of its REST endpoints, allowing any authenticated user (e.g. a customer/subscriber) to retrieve other users' personal data, including their email address, name, and roles.	4.3	More Details
	The updateWorkspace handler in mods/identity/src/workspaces/createUpdateWorkspace.ts in Fonoster		

CVE-2026-80209	through 0.22.7 invokes the gRPC callback with PERMISSION_DENIED when createIsWorkspaceMember reports that the caller is not a member of the target workspace, but it does not return. Execution continues into prisma.workspace.update, which is scoped by the workspace reference alone, so the rename commits before the second callback is issued and the caller receives a permission error for a write that already succeeded. The gRPC interceptor in mods/common/src/identity/createAuthInterceptor.ts binds the workspace accessKeyId to the caller's token only for paths in workspaceResourceAccess or workspaceResourceOwnerOrAdminAccess, and Identity/UpdateWorkspace is listed in fullIdentityAccess, which the base USER role holds. Any authenticated user can therefore rename an arbitrary workspace in the deployment.	4.3	More Details
CVE-2026-80197	Kimai before 2.57.0 contains an improper authorization vulnerability in the favorite timesheet add and remove endpoints that allows authenticated users to manipulate other users' bookmarks. Attackers can add or remove timesheet entries from another user's favorite list by referencing their timesheet identifier, enabling cross-user business-state tampering without administrative privileges.	4.3	More Details
CVE-2026-82625	A vulnerability has been found in code-projects Simple Inventory System 1.0. This affects an unknown part of the file /register.php of the component User Registration. Such manipulation of the argument last_name leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2026-9491	A server-ide request forgery (SSRF) vulnerability in webhook in Synology Chat Server before 2.4.5-22148 allows remote authenticated users to obtain non-sensitive information.	4.3	More Details
CVE-2026-16569	The Mobile App for WooCommerce: ShopApper Mobile App Builder Service for WooCommerce WordPress plugin through 0.4.62 does not check the user's capabilities before allowing a stock-update operation through one of its REST endpoints, allowing any authenticated user, such as a customer or subscriber, to change the stock quantity of arbitrary products.	4.3	More Details
CVE-2026-82809	A security flaw has been discovered in vidIQ Vision for YouTube Extension 3.199.0 on Chrome. The affected element is the function window.addEventListener of the component postMessage Handler. Performing a manipulation of the argument vidiqEvent results in information disclosure. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks. The vendor explains: "At this time, vidIQ does not accept security vulnerability submissions, and we do not have a bug bounty program in place."	4.3	More Details
CVE-2026-82364	A security vulnerability has been detected in macrozheng mall up to 1.0.3. This impacts an unknown function of the file /order/submit of the component Order Submission. The manipulation leads to race condition. It is possible to initiate the attack remotely. The attack is considered to have high complexity. The exploitability is said to be difficult. The vendor deleted the GitHub issue for this vulnerability without and explanation.	4.2	More Details
CVE-2026-59321	A single ScriptEngine instance is reused for every message on a script-backed channel. For JSR-223 engines that report THREADING=null (not thread-safe, e.g. the Kotlin kts engine), concurrent message processing can corrupt engine-internal state, potentially leaking one message's payload/headers bindings into another message's script evaluation or throwing spurious exceptions. Spring Integration 7.1.0 Spring Integration 7.0.0 - 7.0.5 Spring Integration 6.5.0 - 6.5.10 Spring Integration 6.4.0 - 6.4.12 Spring Integration 5.5.21 and earlier	4.2	More Details
CVE-2026-21808	HCL BigFix Quantum Risk Analyzer generates highly detailed logging information by default which increases the risk of sensitive data leakage and can provide an attacker with internal application logic and architectural details.	4.1	More Details
CVE-2026-80488	The WP Ultimate CSV Importer WordPress plugin before 9.0 does not properly sanitise and escape imported field values before using them in a SQL statement, which could allow high privilege users such as admin to perform SQL injection attacks.	4.1	More Details
CVE-2026-81680	openssl_encrypt versions before 1.4.9 fail to authenticate recovery-slot presence in envelope-format encrypted files, allowing attackers to remove recovery slots without re-encrypting the payload. Attackers can modify the file header to delete recovery-slot fields and bypass authentication, silently removing recovery paths the owner deliberately added.	4.0	More Details
CVE-2026-80213	An issue was discovered in the resolv gem before 0.7.2 for Ruby. Resolv::DNS::MessageEncoder wrote a DNS label's length into a single octet without checking its range. A label longer than 255 octets had its length stored modulo 256 but the label data was written unchanged, and thus the bytes on the wire described a different name than the one the application asked to encode. RFC 1035 section 2.3.4 limits a label to 63 octets, and the two high bits of the length octet are reserved for compression pointers. put_string packed the length with put_pack("C", d.length) and put_label used it for labels, and thus any value from 0 to 255 could end up as a label length octet, including the reserved 0x40-0xBF range and the 0xC0-0xFF pointer range. Resolv::DNS::Name.create did not check per-label or total name length either, and thus an attacker-controlled hostname reached the encoder unchanged. An application that resolves an attacker-controlled hostname sends a query whose wire bytes name a domain the attacker chose. A hostname suffix that the application validates against an allowlist becomes padding that never appears on the wire, and thus allowlist and egress checks can be bypassed. The recursive resolver caches the response under the attacker's name,	4.0	More Details

	and DNS logs record that name rather than the one the application asked for. A label length whose low octet lands in the 0xC0-0xFF range produces a length octet that conforming parsers read as the start of a compression pointer, with the following attacker-controlled byte as the offset.		
CVE-2026-21807	HCL BigFix Quantum Risk Analyzer binary lacks several critical, industry-standard hardening protections that could allow an attacker to cause a stack-based buffer overflow.	3.9	More Details
CVE-2026-21809	HCL BigFix Quantum Risk Analyzer has a certain validation process that provides overly descriptive error messages when it encounters malformed input which can allow an attacker to conduct more efficient reconnaissance and fine-tune automated fuzzing tools to produce valid input.	3.9	More Details
CVE-2026-82665	A vulnerability was detected in yaojingang GEOFlow up to 2.1.0. This vulnerability affects the function unlink of the file app/Http/Controllers/Admin/ImageLibraryController.php of the component Image Library Cleanup. The manipulation of the argument file_path results in path traversal. The attack may be performed from remote. The exploit is now public and may be used. Upgrading to version 2.1.1 is able to resolve this issue. The patch is identified as 67abfd864a15d169a78429f3290c91cb3b93e849. It is recommended to upgrade the affected component.	3.8	More Details
CVE-2026-59277	Spring Security's InetAddressMatchers utility provides matchInternal() and matchExternal() builders for constructing an InetAddressMatcher that classifies a given IP address as belonging to an internal (private) or external (public) network. Spring Security 7.1.0	3.7	More Details
CVE-2026-82555	A vulnerability has been found in TOTOLINK N600R 4.3.0cu.7866_B20220506. This vulnerability affects the function loginAuth of the file /web_cste/cgi-bin/cstecgi.cgi of the component Authentication Handler. Such manipulation leads to insufficiently random values. It is possible to launch the attack remotely. This attack is characterized by high complexity. It is stated that the exploitability is difficult. The exploit has been disclosed to the public and may be used.	3.7	More Details
CVE-2026-77063	multer is a middleware for handling multipart/form-data in Node.js. When an application uses an asynchronous fileFilter together with the fileSize limit, a race condition in multer's file stream handling can allow a file that exceeds the configured size limit to bypass the size-limit rejection. All versions before 2.3.0 are affected. The impact is limited because the underlying multipart parser still truncates the stream at the size limit, so this is a bypass of the limit rejection rather than uncontrolled resource consumption. The issue is fixed in multer 2.3.0. Upgrade to multer 2.3.0 to remediate.	3.7	More Details
CVE-2026-47843	In specific scenarios involving multiple clients with different DNS resolver configurations, Reactor Netty may incorrectly reuse a previously configured DNS resolver. Reactor Netty 1.3.0 - 1.3.6 Reactor Netty 1.1.0 - 1.2.18 Reactor Netty 1.0.52 and earlier	3.7	More Details
CVE-2026-19220	The Forminator Forms WordPress plugin before 1.57.1 does not verify that site registration is enabled on the network before creating a site signup, allowing unauthenticated visitors to create a new site on a WordPress multisite network and gain administrator privileges on it.	3.7	More Details
CVE-2026-81725	NLTK before 3.10.3 contains a regular expression denial of service vulnerability in PI196xCorpusReader that allows attackers to cause quadratic CPU consumption by supplying malformed TEI blocks with many unmatched opening tags. Attackers can exploit lazy regex patterns in the read_block method through public APIs like words() and tagged_words() to force repeated rescans and achieve near-quadratic runtime growth.	3.7	More Details
CVE-2026-80199	Kimai before 2.54.0 contains a timing oracle vulnerability in TokenAuthenticator that allows unauthenticated attackers to enumerate valid usernames via X-AUTH-USER header. Attackers can measure response time differences when the password hasher runs only for existing users, enabling username enumeration with no login throttling protection.	3.7	More Details
CVE-2026-81723	NLTK versions before 3.10.3 contain a quadratic CPU exhaustion vulnerability in XMLCorpusView._read_xml_fragment() that rescans accumulated XML fragments on every 1 KiB block read. Attackers can provide malformed XML corpus files to cause severe CPU consumption and denial of service through affected readers like BNCCorpusReader.	3.7	More Details
CVE-2026-82697	A security vulnerability has been detected in sambitraj Student-Management-System up to 56ba287f2e9031523ccb4244cb6e3fe530e4e5d5. The impacted element is the function session_start. Such manipulation leads to cookie without 'httponly' flag. The attack may be launched remotely. A high complexity level is associated with this attack. The exploitability is regarded as difficult. The exploit has been disclosed publicly and may be used. This product operates on a rolling release basis, ensuring continuous delivery. Consequently, there are no version details for either affected or updated releases. The project was informed of the problem early through an issue report but has not responded yet.	3.7	More Details
CVE-2026-59314	Applications that build a Content-Disposition header value from untrusted input may be vulnerable to HTTP response splitting when the input is a malicious file name. Spring Framework 7.0.0 - 7.0.8 Spring Framework 6.2.0 - 6.2.19 Spring Framework 6.1.0 - 6.1.28 Spring Framework 6.0.0 - 6.0.30 Spring Framework 5.3.0 - 5.3.49 Spring Framework 5.2.25.RELEASE and earlier	3.7	More Details
	free5GC is an open-source implementation of the 5G core network. Prior to 1.4.5, the AUSF component performs cryptographic authentication comparisons in internal/sbi/processor/ue_authentication.go with ordinary equality helpers. Auth5gAkaComfirmRequestProcedure compares RES* and XRES* with strings.EqualFold and logs the expected XRES* value at INFO level before comparison.		

CVE-2026-55785	EapAuthComfirmRequestProcedure compares AT_MAC and XMAC with bytes.Equal and evaluates XRES == RES with ordinary string equality. These comparisons can return at mismatch-dependent times, although testing did not demonstrate a practical remote timing oracle because of HTTP/SBI timing noise. The INFO log exposes authentication material to operators, log collectors, sidecars, or processes able to read AUSF logs. This issue is fixed in version 1.4.5.	3.7	More Details
CVE-2025-62341	HCL Connections is vulnerable to server-side request forgery (SSRF) when an internal server is compromised possibly allowing an attacker to send unauthorized requests in certain scenarios leading to information disclosure or security bypass.	3.7	More Details
CVE-2026-13735	Zephyr's WireGuard implementation in subsys/net/lib/wireguard/wg_crypto.c mishandled keepalive packets. In wg_process_data_message(), any type-4 transport-data message whose payload was exactly 16 bytes (an empty plaintext plus a bare Poly1305 tag, i.e. a keepalive) was accepted and returned immediately, before wg_decrypt_packet() was ever called. The Poly1305 authentication tag was therefore never verified; the only preceding gates were a cleartext receiver-index lookup (get_peer_keypair_for_index() on the attacker-supplied data_hdr->receiver) and a non-cryptographic keypair validity/expiry check. The path is reachable entirely from the network: inbound UDP on the WireGuard port is dispatched by wg_input() to handle_transport_data() and then wg_process_data_message(). The 32-bit receiver index is transmitted in cleartext in WireGuard handshake and data messages, so an on-path observer learns it directly and an off-path attacker can brute-force it against the UDP port. Given an active receiving-valid session for that index, an attacker could send a 16-byte garbage payload and have it accepted without possessing the session key. On acceptance the unauthenticated message caused the management layer to observe a spoofed NET_EVENT_VPN_CONNECTED signal (setting peer->first_valid and notifying any net_mgmt listener) and incremented the keepalive-RX statistic. The impact is limited to integrity of this status signal: no plaintext is decrypted or injected, no key is disclosed, and the early-return path did not update the peer endpoint or liveness timers, so there is no traffic-injection, session-takeover, or availability consequence. The fix removes the pre-decrypt early return so a 16-byte payload flows through wg_decrypt_packet(), which verifies the Poly1305 tag over the empty plaintext, followed by the existing anti-replay check; only an authenticated, non-replayed message is then recognised as a keepalive. Forged keepalives now fail the tag check and are counted as decrypt failures.	3.7	More Details
CVE-2026-40203	When IMAP compression is enabled, the same compression state is reused across responses in a session, so response sizes depend on both attacker-supplied mail and other mail in the same mailbox. An attacker that can send mail to a user and can also observe the sizes of that user's IMAP traffic can confirm whether the body of a small message matches a guessed text. Recovery of arbitrary unknown content was not demonstrated, but the attack can disclose whether a secret-like message body matches a candidate. Disable IMAP compression. Update to non-vulnerable version. No publicly available exploits are known.	3.7	More Details
CVE-2026-54713	CakePHP Queue is a queue-interop compatible queueing library. From 0.1.11 until 2.3.1, QueueManager::getUniqueId() generates identifiers for jobs with shouldBeUnique enabled from the job class, method, and parameters, but sorting parameter values drops associative-array keys. An unauthenticated attacker who can influence job parameters can submit semantically different data that produces the same identifier, resulting in legitimate jobs dropped as duplicate collisions. This issue is fixed in version 2.3.1.	3.7	More Details
CVE-2026-82562	### Summary When `qs.parse` is called with `comma: true` and `throwOnLimitExceeded: true`, a comma-separated value under a bracket-push key (`a[]=1,2,3,4`) is split into an array without being compared against `arrayLimit`, while the same value under a flat key (`a=1,2,3,4`), an indexed key (`a[0]=`), a nested key (`a[b]=`), or a dotted key (`a.b=` with `allowDots`) throws the documented `RangeError`. A single parameter such as `a[]=1,2,2,...` therefore produces an inner array of arbitrary length even though the caller opted into the hard limit. This is the `[]=` key form that the fix for CVE-2026-2391 (qs 6.14.2) did not cover. ### Details In `lib/parse.js`, a comma-separated value under a `[]=` key is split and then wrapped as a single nested element (`val = [val]`, so that each `a[]=x,y` group counts as one element of the outer array). The `arrayLimit` check that 6.14.2 added for comma values runs after that wrap, so for `[]=` parts it only ever saw the wrapper of length 1. 6.15.3 added a pre-split comma count so that an oversized value throws before it is allocated, but gated it on an `isFlatArrayValue` flag that `parseValues` set to `false` for any part containing `[]=`, and did not pass it for object-valued input, so the gap remained. #### PoC ```js var qs = require('qs'); var options = { comma: true, arrayLimit: 3, throwOnLimitExceeded: true }; qs.parse('a=1,2,3,4', options); // RangeError: Array limit exceeded. Only 3 elements allowed in an array. qs.parse('a[]=1,2,3,4', options); // { a: [['1', '2', '3', '4']] } (no throw) qs.parse('a[]=' + '1,'.repeat(1000000) + '1', { comma: true, arrayLimit: 20, throwOnLimitExceeded: true }); // no throw; a 1,000,001-element inner array is allocated ``` #### Fix `lib/parse.js`, applied in 8859c37 on `main` and released as v6.16.0: the `isFlatArrayValue` gate is removed, so every comma-split value is counted against `arrayLimit` before splitting regardless of key form. An in-limit group under `a[]=` still counts as one element of the outer array, and the default (`throwOnLimitExceeded: false`) path is unchanged. ### Affected versions `>=6.14.2 <6.16.0`, fixed in v6.16.0. v6.14.2 introduced `arrayLimit` enforcement for comma values (the fix for CVE-2026-2391) but only for values not under a `[]=` key, and every release from v6.14.2 through v6.15.3 has the same gap. v6.14.0 and v6.14.1, where `throwOnLimitExceeded` exists but does not apply to any comma form, are covered by CVE-2026-2391 rather than this record. Earlier lines (6.7.x through 6.13.x) have `comma` but no `throwOnLimitExceeded`, so there is no hard cap on any comma path to bypass; releases before 6.7.0 have no `comma` option. ### Impact An unauthenticated attacker who can reach an application that parses untrusted query strings or urlencoded bodies with both `comma: true` and `throwOnLimitExceeded: true` (both non-default) can bypass the configured limit with a	3.7	More Details

	single `a[]=` parameter and force the parser to allocate an array proportional to the request size. The cost is strictly linear in the attacker-supplied bytes (about 0.1 microseconds and 6 to 7 retained bytes per input byte; the same out-of-memory threshold as the documented default `throwOnLimitExceeded: false` path), so a transport-layer request or body size limit bounds it completely (and node's default maximum HTTP header size of 16 KB already bounds the request line, so multi-megabyte payloads need a body parser). The impact is that an opt-in hard limit fails open on one key spelling, not unbounded allocation from a small input.		
CVE-2026-81836	A vulnerability was detected in RooCodeInc Roo-Code up to 3.51.1. This vulnerability affects unknown code of the file src/integrations/claude-code/oauth.ts of the component OAuth Callback. The manipulation results in cleartext transmission of sensitive information. The attack may be performed from remote. A high complexity level is associated with this attack. It is stated that the exploitability is difficult. The exploit is now public and may be used. Multiple isses were reported to the vendor beforehand. They explain, that "they all apply to Roo Code, a project we no longer support - the repository was archived a while ago, and we don't encourage anyone to use it." This vulnerability only affects products that are no longer supported by the maintainer.	3.7	More Details
CVE-2026-7487	GitLab has remediated an issue in GitLab EE affecting all versions from 13.1 before 19.1.7, 19.2 before 19.2.5, and 19.3 before 19.3.1 that, under certain conditions, an authenticated user with reporter-role permissions who authored a merge request could have reset merge request approval rules due to improper authorization checks.	3.5	More Details
CVE-2026-78364	The MW WP Form WordPress plugin before 5.1.6 does not sanitise and escape some of its form settings before outputting them back in an admin dashboard page, which could allow users with a role as low as Editor to perform Stored Cross-Site Scripting attacks against high privilege users such as admin.	3.5	More Details
CVE-2026-82482	A security vulnerability has been detected in coppermine-gallery Coppermine Photo Gallery up to 1.6.28. This affects an unknown function of the file profile.php of the component edit_profile Endpoint. The manipulation of the argument Biography leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used. Upgrading to version 1.6.29 mitigates this issue. Upgrading the affected component is recommended.	3.5	More Details
CVE-2026-56547	The Apple profile generated for the Apple built-in Mail, Calendar and Contacts account to synchronize with HCL Traveler requires the Logon Name and Mail Address to be embedded in them. The values cannot be changed later on, so the Apple profile generation page asks for those values and reflects them back in the generated Apple profile. The Apple profile is not usable without additional information and only allows the attacker to attack their own device, but HCL Traveler could at least check that the values submitted and reflected back in the Apple profile are found in the Domino directory entry for the already authenticated user.	3.5	More Details
CVE-2026-82483	A vulnerability was detected in coppermine-gallery Coppermine Photo Gallery up to 1.6.28. This impacts an unknown function of the file db_input.php of the component Hidden Album Update Endpoint. The manipulation results in cross site scripting. The attack can be launched remotely. The exploit is now public and may be used. Upgrading to version 1.6.29 will fix this issue. It is recommended to upgrade the affected component.	3.5	More Details
CVE-2026-81848	A vulnerability was determined in cyberchitta scrapling-fetch-mcp up to 0.2.2. The impacted element is the function s_fetch_page/s_fetch_pattern of the file src/scrapling_fetch_mcp/_fetcher.py. Executing a manipulation can lead to server-side request forgery. The attack can be launched remotely. Upgrading to version 0.2.3 is sufficient to resolve this issue. This patch is called 9f6f34e92c55c3d95566ad9c62aca7327d24533a. Upgrading the affected component is advised.	3.5	More Details
CVE-2026-82488	A vulnerability was identified in Beetel 450TC3 01.00.00_01. This vulnerability affects unknown code of the component User Management. The manipulation of the argument Username leads to cross site scripting. The attack is possible to be carried out remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2026-77508	Weblate is a web based localization tool. Prior to 2026.8, an authenticated user can change the account's primary email through PUT or PATCH requests to /api/users/{username}/ without verifying the new address, allowing a later team invitation for that address to be accepted without access to the intended recipient's mailbox. This issue is fixed in version 2026.8.	3.5	More Details
CVE-2026-13416	The CMP WordPress plugin before 4.1.18 does not sanitise and escape a settings value before outputting it on the coming-soon page, allowing users with the Editor role (when the administrator has granted the Editor role access to the CMP WordPress plugin before 4.1.18's admin-bar controls) to inject arbitrary web scripts that execute when a visitor views the page.	3.5	More Details
CVE-2026-77573	Weblate is a web-based continuous localization platform used to manage software translations. In versions prior to 2026.8, a user permitted to manage component repository URLs can perform server-side request forgery against internal services through DNS rebinding during VCS operations. Weblate validates the hostname's first DNS resolution, but the external VCS clients that later connect perform a separate DNS lookup, so an attacker-controlled hostname that initially resolves to a public address can be re-pointed to an internal or private address before the connection is made. By triggering a clone, fetch, push, or similar remote operation, the attacker can cause Weblate to reach internal VCS-compatible services and potentially	3.5	More Details

	expose private repository contents. Installations that permit untrusted repository hostnames while using VCS_RESTRICT_PRIVATE=True are affected. This issue is fixed in version 2026.8.		
CVE-2026-82112	A flaw has been found in houtini-ai houtini-lm up to 2.13.2. The impacted element is an unknown function of the file src/index.ts of the component code_task_files. Executing a manipulation can lead to path traversal. The attack can be launched remotely. This patch is called 35d97bca0531894da36a85aedb95312da1bd5b7a. It is best practice to apply a patch to resolve this issue.	3.5	More Details
CVE-2026-81717	openssl_encrypt (pip package openssl-encrypt) before 1.4.9 contains two weaknesses in the portable USB drive feature, whose threat model treats the removable drive as untrusted (attacker with physical write access). USBDriveCreator._verify_integrity_file only validates files listed in the manifest, so files added to the drive — including a root-level autorun payload — are not detected and integrity verification still passes. Additionally, a globally constant, source-embedded KDF salt (_LEGACY_FIXED_SALT) is used to derive the drive encryption key for any drive lacking a per-drive salt file, defeating precomputation resistance and enabling an offline rainbow-table attack.	3.5	More Details
CVE-2026-82622	A security vulnerability has been detected in code-projects Employee Leave Managing System 1.0. Affected is an unknown function of the file /EmpManageSys/editaction.php of the component Employee Profile Update. The manipulation of the argument Name leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used.	3.5	More Details
CVE-2026-82671	A vulnerability has been found in IObit Unlocker 1.3.0.12. This vulnerability affects the function ZwTerminateProcess in the library IObitUnlocker.sys of the component IRP_MJ_DEVICE_CONTROL Handler. The manipulation leads to improper privilege management. An attack has to be approached locally. The vendor was contacted early about this disclosure but did not respond in any way.	3.4	More Details
CVE-2026-82810	A weakness has been identified in extension.vn 2FA Authenticator Extension 1.0.0.2 on Chrome. The impacted element is the function chrome.runtime.onMessageExternal.addListener of the component Background Service Worker. Executing a manipulation of the argument sender.id can lead to information disclosure. The attack requires local access. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure.	3.3	More Details
CVE-2026-54548	kas is a setup tool for bitbake based projects. Prior to 5.4, internal SSH key setup triggered by SSH_PRIVATE_KEY or SSH_PRIVATE_KEY_FILE creates ~/.ssh/config when no user-specific SSH configuration exists and adds a global Host * rule containing StrictHostKeyChecking no. In kas/libcmds.py, ssh_no_host_key_check() runs without checking ctx.managed_env, so the setting persists after kas exits and affects future SSH sessions by the same local user, extending beyond the intended short-lived continuous integration environment. A later SSH connection can therefore accept an attacker-controlled host key without verification, increasing the risk of a man-in-the-middle attack that compromises session confidentiality or integrity. This issue is fixed in version 5.4.	3.3	More Details
CVE-2026-38093	file_picker (aka flutter_file_picker) for Flutter, all versions through 10.3.10, is vulnerable to path traversal (CWE-22) in its Android implementation. The openFileStream() method in FileUtils.kt uses the DISPLAY_NAME obtained from ContentResolver.query() directly in file path construction without sanitization. A malicious Android app with a crafted ContentProvider can return a filename containing ../ sequences, causing the plugin to create arbitrary files and directories outside the intended cache directory within the victim app's internal storage. Existing files are not overwritten due to an existence check.	3.3	More Details
CVE-2026-81696	openssl_encrypt versions before 1.4.9 fail to sanitize terminal control characters in file metadata printed by the info command. Attackers can craft malicious files containing escape sequences to repaint terminal output and forge verification information displayed to users.	3.3	More Details
CVE-2026-81695	openssl_encrypt versions before 1.4.9 fail to escape attacker-controlled key_id values printed to stderr during decrypt auto-detection. Attackers can craft encrypted files with malicious key_id containing escape sequences to repaint terminal output and forge authenticity verification blocks.	3.3	More Details
CVE-2026-81715	openssl_encrypt (pip package openssl-encrypt) versions <= 1.4.8 do not redact the keyserver bearer token passed as the positional argument to 'keyserver set-token' in the --debug argv dump, because sanitize_argv_for_debug fails to sanitize it. As a result the token is printed in cleartext to stderr under --debug (even without --unsafe-show-secrets), persisting the credential in logs and terminal history. Fixed in 1.4.9.	3.3	More Details
CVE-2026-81694	openssl-encrypt (pip package, versions <= 1.4.8) fails to sanitize filenames read from untrusted drive data (outside the AES-GCM authenticated manifest) before printing them in the verify-usb command's output. An attacker can plant filenames containing terminal cursor-movement and erase-line control bytes that repaint a forged PASSED verdict on screen, masking actual tamper detection. Fixed in 1.4.9 by routing drive-derived names through sanitize_for_display().	3.3	More Details
CVE-2026-81685	openssl_encrypt versions before 1.4.9 fail to sanitize recovery-slot metadata in the desktop GUI, allowing attackers to inject control characters and line separators into the irreversible-removal confirmation dialog. Attackers can craft encrypted files with malicious slot identifiers containing bidi overrides or line-separator characters to forge warning text and deceive users during file removal operations.	3.3	More Details
CVE-2023-	A malicious virtual function can invoke the certain command handlers in the SMU, causing a denial of	3.3	More

31308	service due to out-of-bounds memory read.		Details
CVE-2026-82596	A vulnerability was determined in LatencyUtils up to 2.0.3. Affected by this issue is the function LatencyStats.recordDetectedPause of the file src/main/java/org/LatencyUtils/LatencyStats.java of the component PauseDetector. Executing a manipulation can lead to memory corruption. The attack needs to be launched locally. 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.	3.3	More Details
CVE-2026-82863	@hulumi/baseline versions before 1.3.2 fail to fully detect CloudTrail selector tampering events, reducing audit logging configuration change coverage. Attackers can modify CloudTrail event selectors without complete detection, potentially evading audit trail monitoring.	3.3	More Details
CVE-2026-59292	PropertiesPersistingMetadataStore, the default file-based ConcurrentMetadataStore, persists its state to ${java.io.tmpdir}/spring-integration/metadata-store.properties with world-readable permissions. Spring Integration 7.1.0 Spring Integration 7.0.0 - 7.0.5 Spring Integration 6.5.0 - 6.5.10 Spring Integration 6.4.0 - 6.4.12 Spring Integration 5.5.21 and earlier	3.2	More Details
CVE-2026-59300	Potential for logging sensitive data in Spring Cloud Function AWS. Spring Cloud Function 5.0.0 - 5.0.3 Spring Cloud Function 4.3.0 - 4.3.4 Spring Cloud Function 4.2.0 - 4.2.7 Spring Cloud Function 3.2.16 and earlier	3.1	More Details
CVE-2026-52681	Sieve CPU resource usage is tracked in the compiled script, so an attacker that has valid credentials can reset the accounting by repeatedly changing the active script. Compiled script files are also not removed when a script is deleted or renamed. The configured Sieve CPU limit can be bypassed, allowing sustained CPU consumption, and the leftover files increase disk consumption. Both can cause degradation of service for mail delivery. Monitor system for abnormal CPU usage and disk consumption. Update to non-vulnerable version. No publicly available exploits are known.	3.1	More Details
CVE-2026-82236	File Browser versions from 2.63.6 through 2.63.23 fail to clean up public share links when a privileged user deletes another user's shared file. Attackers can access the surviving share link to retrieve new unrelated content uploaded to the same path without authentication.	3.1	More Details
CVE-2026-82237	filebrowser through 2.63.23 does not remove share records when a shared file is renamed (only deletion triggers share cleanup). The share record is keyed by path, so it survives the rename and remains dormant (returning 404 while the path is empty). When any new, unrelated file later appears at the original shared path — via re-upload, another user with create permission, or a hook — the stale public share link serves that new file under the original link's password and expiry settings, unexpectedly exposing it.	3.1	More Details
CVE-2026-59301	Potential for logging sensitive data in Spring Cloud Function Azure. Spring Cloud Function 5.0.0 - 5.0.3 Spring Cloud Function 4.3.0 - 4.3.4 Spring Cloud Function 4.2.0 - 4.2.7	3.1	More Details
CVE-2025-62343	HCL IntelliOps Event Management (IEM) is affected by an Admin Session Concurrency Vulnerability. it may allows user sessions to remain active after logout or session deletion.	3.1	More Details
CVE-2026-40204	None None None No publicly available exploits are known.	3.1	More Details
CVE-2026-82238	filebrowser from version 2.24.0 contains a race condition in the TUS upload handler that allows authenticated users to write past the declared Upload-Length by sending concurrent PATCH requests. Attackers can send multiple simultaneous PATCH requests at the same offset to bypass length validation, resulting in files that exceed their declared size and triggering completion hooks for oversized uploads.	3.1	More Details
CVE-2026-42393	The comparison used for the doveadm password and API key is not fully timing safe and can reveal the length of the configured secret. An attacker with access to the same network as the doveadm service, able to make repeated requests and measure response timing accurately, can learn the length of the secret, which reduces the effort needed to guess it. The secret value itself is not disclosed. Restrict network access to the doveadm service to trusted clients. Update to non-vulnerable version. No publicly available exploits are known.	3.1	More Details
CVE-2026-59299	Composition lookup can potentially poison base function in Spring Cloud Function. Spring Cloud Function 5.0.0 - 5.0.3 Spring Cloud Function 4.3.0 - 4.3.4 Spring Cloud Function 4.2.0 - 4.2.7 Spring Cloud Function 3.2.16 and earlier	3.1	More Details
CVE-2026-59302	Potential for logging sensitive data in Spring Cloud Stream. Spring Cloud Stream 5.0.0 - 5.0.2 Spring Cloud Stream 4.3.0 - 4.3.3 Spring Cloud Stream 4.2.0 - 4.2.6	3.1	More Details
CVE-2026-59297	Implementation of isSecure() call of ServerlessHttpServletRequest does not verify the actual scheme. Spring Cloud Function 5.0.0 - 5.0.3 Spring Cloud Function 4.3.0 - 4.3.4 Spring Cloud Function 4.2.0 - 4.2.7	3.1	More Details
CVE-2026-82249	gitoxide before 0.38.2 fails to validate carriage return characters in URL values passed to credential helpers. Attackers can supply URLs containing bare carriage returns to inject additional helper protocol fields and cause credential helpers to return credentials for attacker-specified hosts instead of the requested URL.	3.1	More Details
CVE-2026-59298	Potential for improper filtering of HTTP headers in Spring Cloud Function. Spring Cloud Function 5.0.0 - 5.0.3 Spring Cloud Function 4.3.0 - 4.3.4 Spring Cloud Function 4.2.0 - 4.2.7 Spring Cloud Function 3.2.16 and earlier	3.1	More Details

CVE-2026-14367	The I3C IBI subsystem in drivers/i3c/i3c_ibi_workq.c hands out statically-allocated work nodes through a free-list i3c_ibi_work_nodes_free implemented as a plain sys_slist_t, which provides no synchronization. The allocation helpers (i3c_ibi_work_enqueue, i3c_ibi_work_enqueue_target_irq, i3c_ibi_work_enqueue_hotjoin, i3c_ibi_work_enqueue_controller_request, i3c_ibi_work_enqueue_cb) called sys_slist_get() directly from ISR context, while the workqueue handler i3c_ibi_work_handler() returned nodes with sys_slist_append() from the workqueue thread, with no lock on either side. Because sys_slist_get() and sys_slist_append() are neither atomic nor interrupt-safe, an IBI interrupt that fires while the workqueue thread is mid-append (or a truly parallel access under CONFIG_SMP) races on the shared list. This corrupts the list linkage: a node may be handed to two consumers, a node may be lost, or the head/tail pointers may be left inconsistent so sys_slist_get() returns a stale or garbage pointer. In the double-hand-out case the subsequent memcpy(ibi_node, ibi_work, sizeof(*ibi_node)) overwrites a node still in flight; a garbage pointer turns the same memcpy into an out-of-bounds write. The race is driven by I3C bus traffic — IBIs, hot-joins, and controller-role requests originate from target devices on the bus, and I3C supports hot-joining devices. An attacker controlling an I3C peripheral on the board's chip-to-chip bus can generate high-frequency interrupts timed to collide with the free operation. Exploitation requires physical access to the bus and winning a narrow timing window; the most realistic impact is a crash or hang (denial of service), with memory corruption possible but hard to control. The fix wraps all free-list sys_slist_get()/sys_slist_append() operations in the new ibi_work_alloc()/ibi_work_free() helpers, each guarded by a k_spinlock (ibi_work_lock), closing the race across ISR and thread contexts.	3.1	More Details
CVE-2026-59306	Potential for deserialization of untrusted types in Spring Cloud Stream. Spring Cloud Stream 5.0.0 - 5.0.2 Spring Cloud Stream 4.3.0 - 4.3.3 Spring Cloud Stream 4.2.0 - 4.2.6	3.1	More Details
CVE-2026-59304	Improper caching of the original content type in Spring Cloud Stream Avro. Spring Cloud Stream 5.0.0 - 5.0.2 Spring Cloud Stream 4.3.0 - 4.3.3 Spring Cloud Stream 4.2.0 - 4.2.6	3.1	More Details
CVE-2026-21827	HCL Connections is vulnerable to an information disclosure vulnerability which could allow a user to obtain sensitive information they are not entitled to, caused by improper handling of request data they are not entitled to, caused by improper handling of request data.	3.1	More Details
CVE-2026-13479	The LoRaWAN application-layer clock-synchronization service parses downlinks in clock_sync_package_callback() (subsys/lorawan/services/clock_sync.c). Its command loop only guarantees that the one-byte command id is in bounds; for the CLOCK_SYNC_CMD_APP_TIME (AppTimeAns) command the handler then reads a 4-byte time correction via sys_get_le32() plus a 1-byte token without checking that 5 bytes remain in the receive buffer (len - rx_pos). A short or crafted AppTimeAns therefore reads up to 5 bytes past the end of the decrypted payload. The payload (rx_buf/len) is the decrypted application frame delivered to the registered downlink callback (mcps_indication->Buffer/BufferSize). Reaching the handler requires a frame on the clock-sync port that passes LoRaWAN's MAC integrity check and FRMPayload decryption, so the practical attacker is a malicious or compromised network/application server (the designated sender of AppTimeAns) or a party holding the session keys, rather than an arbitrary radio listener. The over-read is bounded: the backing store is a fixed 255-byte static buffer, so the few stray bytes do not fault, and the read values (time_correction, token) are used only internally and never transmitted, so there is no disclosure to the attacker and no crash. The sole effect is that a stale token matching ctx.req_token can apply a garbage time_correction to the device's own clock offset (ctx.time_offset), a minor integrity impact confined to the victim's time estimate. The fix adds an explicit length check that drops a too-short AppTimeAns. Note the sibling one-byte reads in the periodicity and force-resync handlers remain unguarded with the same negligible impact.	3.1	More Details
CVE-2026-59305	Partition interceptor may be improperly added while sending message. Spring Cloud Stream 5.0.0 - 5.0.2 Spring Cloud Stream 4.3.0 - 4.3.3 Spring Cloud Stream 4.2.0 - 4.2.6	3.1	More Details
CVE-2026-13480	The LoRaWAN TS004 Fragmented Data Block Transport handler frag_transport_package_callback() in subsys/lorawan/services/frag_transport.c parses downlink command bytes without validating that enough payload bytes remain before each access. The loop's only bound is rx_pos < len; after consuming the one-byte command id the handler cast rx_buf + rx_pos to a 10-byte struct frag_transport_setup_req, and for a DATA_FRAGMENT command passed &rx_buf[rx_pos] to the fragment decoder, which reads exactly ctx.frag_size bytes — with no remaining-length check in either case. The fragment size is attacker-chosen in a preceding FRAG_SESSION_SETUP command (ctx.frag_size = req->frag_size, capped at CONFIG_LORAWAN_FRAG_TRANSPORT_MAX_FRAG_SIZE, default 232). rx_buf aliases the 255-byte static MacCtx.RxPayload buffer in the loramac-node MAC layer, while len is the actual decrypted payload length. By padding a downlink with mismatched-index DATA_FRAGMENT filler commands (each advancing rx_pos by three bytes without producing an answer) and appending one matching-index fragment near the end of the payload, an attacker can make the decoder read up to roughly frag_size bytes past the end of RxPayload, copying adjacent static memory into the decoder buffers and the FUOTA flash image. The handler runs only on downlinks that have already passed the LoRaWAN frame MIC and FRMPayload decryption, so the defect is reachable only by a party holding the device's session keys (the FUOTA server or an attacker who has compromised those keys). The out-of-bounds bytes are never returned to the sender — the only uplink emitted is a status answer carrying fragment counts — so there is no direct disclosure channel, and on typical flat-memory LoRaWAN MCUs the over-read stays within mapped memory, making a crash unlikely. The impact is therefore a bounded out-of-bounds read with limited confidentiality consequence and no write or control-flow primitive. The fix adds remaining-length guards before each access.	3.1	More Details
CVE-2026-	Dynamic destination cache size is not properly bound in Spring Cloud Stream. Spring Cloud Stream 5.0.0 -	3.1	More

59303	5.0.2 Spring Cloud Stream 4.3.0 - 4.3.3 Spring Cloud Stream 4.2.0 - 4.2.6		Details
CVE-2026-81102	The Dash MCP server bound its listener to the loopback address but never checked the host a request named. src/mcp_server_dash.py constructed the server for its network mode with the interface restricted to loopback and no transport-security settings, so a name that had been pointed at the loopback address still reached the listener while carrying the attacker's host name. A page in a visitor's browser could therefore drive the local server and invoke its company-search and file-detail tools under the Dropbox credential the server holds. Only the network mode was reachable this way; the standard input mode was not. The fix supplies transport-security settings that enable host checking and allow only the loopback name and port, rejecting other hosts before a tool runs. The repository publishes no versions, so the affected boundary is the commit preceding the fix.	3.1	More Details
CVE-2026-77704	The Booking for Appointments and Events Calendar WordPress plugin before 2.4.9 does not check that a user holds the required capability before letting them change an appointment's status, allowing customers to set arbitrary statuses on appointments they are booked on, including approving their own bookings that were left awaiting approval and overwriting another customer's booking status on a shared appointment.	2.7	More Details
CVE-2026-81200	The MasterStudy LMS WordPress Plugin WordPress plugin before 3.7.42 does not correctly restrict access to order information, allowing any user with the instructor role to read other users' order billing details, including name, email address, phone number and postal address, by enumerating order IDs.	2.7	More Details
CVE-2026-82699	A flaw has been found in sambitraj Student Management System up to 56ba287f2e9031523ccb4244cb6e3fe530e4e5d5. This impacts an unknown function of the file aca.sql of the component Password Handler. Executing a manipulation of the argument Password can lead to cleartext storage of sensitive information. The attack can be executed remotely. The exploit has been published and may be used. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable.	2.7	More Details
CVE-2026-79615	The Quiz and Survey Master (QSM) WordPress plugin before 11.2.4 does not check authorisation when returning question bank entries through one of its REST API routes, allowing users with a role as low as Contributor to read the questions, hints and correct answer keys of quizzes belonging to other users.	2.7	More Details
CVE-2026-9805	SMM IHISI command handler, FMTSWriteUseIntelLib, for FMTS command 0x32, read and write data without checking buffer size and could cause buffer overflow.	2.7	More Details
CVE-2026-82656	Admidio before 5.0.12 fails to sanitize album names in the photo ZIP download functionality, allowing authenticated users with album-creation rights to include path traversal segments in archive entry names. Attackers can craft malicious album names containing directory traversal sequences that escape the intended directory when recipients extract the archive, potentially writing files outside the target directory.	2.6	More Details
CVE-2026-82677	A vulnerability was determined in valkey-io valkey 9.1.0. Impacted is the function moduleTimerHandler of the file src/module.c of the component Module Timer Subsystem. This manipulation causes double free. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized. Patch name: b349fe2821e3998534b1454c1b64a478daf8c6b7. To fix this issue, it is recommended to deploy a patch.	2.4	More Details
CVE-2026-82631	A security flaw has been discovered in valkey-io valkey 9.1.0. The affected element is the function handleClientsBlockedOnKey of the file src/blocked.c of the component Blocked-on-keys Subsystem. The manipulation results in use after free. The attack may be performed from remote. A high complexity level is associated with this attack. The exploitability is described as difficult. The exploit has been released to the public and may be used for attacks. The patch is identified as b2fb0e13f5b4c8c2fb63dcfc2c37a067a0d6d20b. Applying a patch is advised to resolve this issue.	2.2	More Details
CVE-2026-80201	Kimai before 2.53.0 fails to block sensitive User methods in the Twig invoice template sandbox, allowing admins to call getApiToken() and getPlainApiToken() methods. Attackers with template creation permissions can embed these method calls in invoice templates to leak hashed API tokens in rendered invoice output.	2.0	More Details
CVE-2026-59291	Potential arbitrary file read and SSRF vulnerability in Spring Cloud Function. Spring Cloud Function 5.0.0 - 5.0.3 Spring Cloud Function 4.3.0 - 4.3.4 Spring Cloud Function 4.2.0 - 4.2.7	2.0	More Details
CVE-2026-55891	PrivateBin is an online pastebin where the server has zero knowledge of pasted data. Prior to 2.0.5, Request::getRequestUri() in lib/Request.php passes $_SERVER['REQUEST_URI'] through FILTER_SANITIZE_URL, which does not remove quotation marks, angle brackets, or apostrophes, and Controller::_init() stores the attacker-controlled value in Controller::$_urlBase. Controller::_jsonld() in lib/Controller.php then uses str_replace() to insert that value without JSON escaping into js/types.jsonld, js/paste.jsonld, and the other JSON-LD templates used by /?jsonld= and /?pasteid. A raw quotation mark delivered by an HTTP client, proxy, or structured-data crawler that does not normalize the request target can break out of the JSON string and inject arbitrary key-value data into a CORS-open application/ld+json response. The jsonld branch in Controller::__construct() returns before _setCacheHeaders(), so the response also lacks X-Content-Type-Options: nosniff, Content Security Policy, X-Frame-Options, and Referrer-Policy. Direct script execution was not demonstrated, but manipulated responses can affect structured-data consumers or combine with less strict clients. This issue is fixed in version 2.0.5.	0.0	More Details
	In the Linux kernel, the following vulnerability has been resolved: gpio: ml-ioh: use raw_spinlock_t for the register lock ioh_irq_type() is registered as the irq_chip .irq_set_type callback and takes chip->spinlock with		

CVE-2026-80562	spin_lock_irqsave(). This callback is reached from __setup_irq() -> __irq_set_trigger() -> chip->irq_set_type() while the caller holds desc->lock, a raw_spinlock_t, with hardirqs disabled. That context is not sleepable, but on PREEMPT_RT a regular spinlock_t is an rtmutex-backed sleeping lock, so acquiring it there is invalid. ioh_irq_enable() and ioh_irq_disable() take the same lock from the .irq_enable/.irq_disable callbacks, which are likewise invoked with desc->lock held. Convert the register lock to raw_spinlock_t. The same lock also serializes the GPIO direction/value callbacks and the suspend/resume register save/restore, and those critical sections only perform short sequences of MMIO register accesses (ioread32()/iowrite32()); the .irq_set_type callback additionally emits a dev_warn() on an unsupported type. None of these are sleepable operations, so keeping this register lock non-sleeping is appropriate for the irqchip callbacks and does not change the GPIO-side locking contract. This is the same fix as commit a02b8950d619 ("gpio: pch: use raw_spinlock_t for the register lock"); this driver shares the same structure as gpio-pch.	N/A	More Details
CVE-2026-63083	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-51705	Incorrect access control in the setWiFiMeshName function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to rename mesh entries via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	N/A	More Details
CVE-2026-78422	Subject::new_for_owner() in the zbus_polkit crate encodes the uid entry of a unix-process polkit subject as an unsigned 32-bit integer (D-Bus type u), whereas the org.freedesktop.PolicyKit1.Authority interface specifies a signed 32-bit integer (D-Bus type i). Because of this type mismatch, polkit silently discards the caller-supplied UID and instead determines the subject's owner itself by looking up the PID in /proc, a lookup that is inherently subject to a time-of-check/time-of-use race. Consequently, an application that passes a UID obtained from a trustworthy source — for example SO_PEERCRED Unix socket peer credentials — in order to defend against PID reuse receives no protection, and the supplied UID has no effect on the authorization decision. A local unprivileged attacker who can cause an authorized process to terminate and then win the race to have their own process assigned the same PID can be authorized under the identity of the terminated process, bypassing the polkit authorization check and performing actions the attacker is not entitled to. This issue affects zbus_polkit before 5.1.0.	N/A	More Details
CVE-2026-75062	Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') in the default lf.query Python protocol in Google langfun versions prior to 0.1.2 allows remote unauthenticated attackers to execute arbitrary Python code in the context of the host application via crafted prompt inputs that cause the model to generate executable Python expressions evaluated without a sandbox.	N/A	More Details
CVE-2026-82823	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2026-82814. Reason: This candidate is a reservation duplicate of CVE-2026-82814. Notes: All CVE users should reference CVE-2026-82814 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2026-83492	Improper input validation vulnerability in Extend Themes Kubio AI Website Builder. This issue affects Kubio AI Website Builder: before 2.9.1.	N/A	More Details
CVE-2026-80216	Rejected reason: duplicate record	N/A	More Details
CVE-2026-51738	Incorrect access control in the LoadDefSettings function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to reset the device configuration and reboot the device via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	N/A	More Details
CVE-2026-80214	LibreNMS’s Virtualization Discovery module is vulnerable to command line injection. An authenticated admin user can execute arbitrary code on the host server.	N/A	More Details
CVE-2026-54599	Wallos is an open-source, self-hostable personal subscription tracker. Prior to version 4.9.4, login.php generates an OIDC state nonce stored in $_SESSION['oidc_state'], but checksession.php dispatches the OIDC callback without comparing the incoming state against the session value. An attacker can trick a victim into visiting a crafted URL, causing Wallos to exchange the attacker's authorization code and log the victim into the attacker's account. This issue has been patched in version 4.9.4.	N/A	More Details
CVE-2026-54600	Wallos is an open-source, self-hostable personal subscription tracker. Prior to version 4.9.4, endpoints/db/import.php has no authentication. The only guard is a user-table row count — if zero (fresh/unconfigured install), an unauthenticated attacker can replace the entire database. This issue has been patched in version 4.9.4.	N/A	More Details
CVE-2026-80577	In the Linux kernel, the following vulnerability has been resolved: drm/panthor: skip zero-sized firmware sections panthor_fw_load_section_entry() skips BO creation when the firmware section VA range is empty. If such a section is added to the firmware section list, section->mem is left as NULL. Later reload and unplug paths iterate over all firmware sections and dereference section->mem, which can lead to a NULL pointer dereference. Zero-sized firmware sections are valid, so accept them as no-op entries but skip adding them to the section list.	N/A	More Details
CVE-2026-	Wallos is an open-source, self-hostable personal subscription tracker. Prior to version 4.9.6, POST /endpoints/notifications/testemailnotifications.php accepts smtpaddress and smtpport from POST body with zero SSRF validation. PHPMailer connects to attacker-supplied host:port. Every other notification endpoint	N/A	More

61638	uses ssrf_helper.php but email was missed. Any authenticated user can probe internal network, cloud metadata. This issue has been patched in version 4.9.6.		Details
CVE-2026-61639	Wallos is an open-source, self-hostable personal subscription tracker. Prior to version 4.9.6, POST /endpoints/db/restore.php calls ZipArchive::extractTo() without validating entry names for ../ sequences. Admin uploads crafted zip with entry logos/../../endpoints/shell.php to write webshell to webroot. Extension filter only applies to post-extraction logo copy step. This issue has been patched in version 4.9.6.	N/A	More Details
CVE-2026-61640	Wallos is an open-source, self-hostable personal subscription tracker. Prior to version 4.9.6, Admin-configured OIDC token_url and user_info_url in includes/oidc/handle_oidc_callback.php:18-49 are used directly in curl_init() with zero SSRF filtering. Unlike logo/webhook URLs which have validate_webhook_url_for_ssrf(), OIDC URLs bypass all protections. Admin sets URL to http://169.254.169.254/latest/meta-data/ for cloud metadata access or internal network pivoting. This issue has been patched in version 4.9.6.	N/A	More Details
CVE-2026-62993	Smarty is a template engine for PHP, facilitating the separation of presentation (HTML/CSS) from application logic. Prior to 4.5.7 and 5.8.2, depending on the release line, Smarty's {fetch} handling in libs/plugins/function.fetch.php and src/FunctionHandler/Fetch.php used Security::isTrustedUri() to validate only the initial remote URL against trusted_uri when a security policy was active. For resources handled by file_get_contents(), including HTTPS URLs, PHP followed HTTP redirects by default. An attacker who could supply or influence a fetch target and had an open redirect on a trusted host could redirect the request to an attacker-chosen internal endpoint, bypass the trusted_uri allowlist, and perform server-side request forgery. This issue is fixed in versions 4.5.7 and 5.8.2.	N/A	More Details
CVE-2026-71415	Kirby is an open-source content management system. From 5.0.0 until 5.5.2, Kirby's REST API chunk upload handler in src/Api/Upload.php did not run the relevant upload authorization preflight in Kirby\Api\Upload::process() before Kirby\Api\Upload::processChunk() persisted chunk data. An authenticated user with the access.panel permission enabled but with files.create, files.replace, and user/users.update permissions disabled could submit requests with an Upload-Length header and leave unfinished chunks in site/cache/.uploads for 24 hours. Repeating this process could consume attacker-controlled temporary storage, prevent other users from uploading files, or prevent site logic from storing data, although final permission checks still prevented unauthorized files from reaching the content or site/accounts directories. This issue is fixed in version 5.5.2.	N/A	More Details
CVE-2026-75592	Kirby is an open-source content management system. Prior to 4.9.5 and 5.5.2, depending on the release line, Kirby's media handler used incomplete filesystem containment checks in src/Filesystem/Dir.php and src/Filesystem/F.php through Kirby\Filesystem\Dir::realpath() and Kirby\Filesystem\F::realpath(). The checks accepted a sibling directory whose path shared the intended root's string prefix, such as /var/www/site2 next to /var/www/site, because they did not require an exact match or a DIRECTORY_SEPARATOR boundary. A remote attacker could use Kirby\Cms\Media::thumb() to create and access thumbnails from image files in a PHP-readable sibling directory when that directory contained a valid .json thumbnail job file, potentially exposing staging sites, backups, or other internal sites and deleting the job file during processing. This issue is fixed in versions 4.9.5 and 5.5.2.	N/A	More Details
CVE-2026-75594	Kirby is an open-source content management system. Prior to 4.9.5 and 5.5.2, depending on the release line, Kirby's media handler in src/Cms/Media.php allowed Kirby\Cms\Media::thumb() to append a path-bearing filename to a validated parent media directory. On nginx, PHP's built-in server, or Apache with AllowEncodedSlashes enabled, a remote attacker could submit encoded slash characters such as %2f in the filename and traverse outside the parent's media directory. Differences between responses for existing and nonexistent thumbnail configurations disclosed whether an arbitrary .json file existed, and a .json file containing a valid filename key could cause the referenced image to be returned and the job file to be deleted. The related file::version path in src/Filesystem/Asset.php also accepted ../ sequences outside the intended index root. This issue is fixed in versions 4.9.5 and 5.5.2.	N/A	More Details
CVE-2026-80725	In the Linux kernel, the following vulnerability has been resolved: net: gro: properly validate BIG TCP aggregation criteria When GRO attempts to aggregate packets beyond GRO_LEGACY_MAX_SIZE (64KB), BIG TCP should only be permitted for plain IPv4 TCP and plain IPv6 TCP (with sufficient MAC header room to insert the temporary HBH jumbo header). However, commit b1a78b9b9886 ("net: add support for ipv4 big tcp") loosened the check in skb_gro_receive(), leading to several issues: 1. skb_gro_receive() checked skb_headroom(p) instead of the actual space before the MAC header (p->mac_header). Because skb_headroom(p) includes mac_len, crafted frames (e.g. injected via AF_PACKET) can pass the check with p->mac_header < 8 bytes. When ipv6_gro_complete() inserts the temporary HBH jumbo header, the memmove() starts before skb->head, causing an out-of-bounds write and wrapping skb->mac_header. 2. It allowed non-IP protocols such as software VLAN (ETH_P_8021Q / ETH_P_8021AD) to aggregate beyond 64KB because p->protocol != ETH_P_IPV6 was true. 3. It checked p->encapsulation instead of NAPI_GRO_CB(skb)->encap_mark, allowing encapsulated flows (e.g. SIT / IPv6-in-IPv4) to aggregate beyond 64KB. Fix skb_gro_receive() to strictly enforce: - NAPI_GRO_CB(skb)->proto == IPPROTO_TCP - Not encapsulated (!NAPI_GRO_CB(skb)->encap_mark && !p->encapsulation) - Protocol must be either ETH_P_IP or ETH_P_IPV6 - If ETH_P_IPV6, p->mac_header must be at least sizeof(struct hop_jumbo_hdr) Returning -E2BIG from skb_gro_receive() ensures that packets which cannot become BIG TCP are cleanly flushed at <= 64KB and delivered intact without dropping. This issue does not exist in mainline (7.0+) because the subsystem was rewritten in commit 81be30c1f5f2 ("net/ipv6: Drop HBH for BIG TCP on RX side"), making this fix relevant only for older stable branches like 6.18.y.	N/A	More Details

CVE-2026-76149	CorvusSKK contains an integer overflow vulnerability, which may allow malicious data to be written to a dictionary file.	N/A	More Details
CVE-2026-76148	CorvusSKK contains a code injection vulnerability, which may lead to arbitrary code execution on the affected product.	N/A	More Details
CVE-2026-73335	Android application "Myna Point" is vulnerable to Improper Authorization in Handler for Custom URL Scheme (CWE-939). A malicious application installed on the user's Android device may exploit the affected application's functionality through an Intent, potentially allowing arbitrary JavaScript to be executed within the affected application.	N/A	More Details
CVE-2026-51733	Incorrect access control in the FirmwareUpgrade function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to remove Wi-Fi schedule entries via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	N/A	More Details
CVE-2026-9146	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-9250	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-80564	In the Linux kernel, the following vulnerability has been resolved: gve: fix NULL dereference due to missing ptp adjfine Fix NULL dereference due to missing implementation of adjfine, which can be triggered from usermode as follows: sudo ./testptp -d /dev/ptp0 -f 0 [551.943697] BUG: kernel NULL pointer dereference, address: 0000000000000000 [...] [552.061946] Call Trace: [552.064487] <TASK> [552.066681] ptp_clock_adjtime+0x1c0/0x2c0 [552.070874] ? get_clock_desc+0x6b/0xb0 [552.074825] pc_clock_adjtime+0x78/0xc0 [552.078755] __do_sys_clock_adjtime+0x85/0x110 [552.083293] do_syscall_64+0xea/0x610	N/A	More Details
CVE-2026-51723	Incorrect access control in the UploadCustomModule function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to install a custom CGI module via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	N/A	More Details
CVE-2026-15203	Improper access control in debug and engineering interfaces in Danfoss iC7-Automation SP, iC7-Marine, and iC7-Hybrid GR3 allows attackers to gain read/write access to internal values, upload and execute unsigned applications, and upload unsigned EEPROM data and firmware via exposed service interfaces and software update mechanisms	N/A	More Details
CVE-2026-51728	Incorrect access control in the UploadFirmwareFile function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to upload a crafted firmware image via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	N/A	More Details
CVE-2026-79743	MCPHub is a unified hub for centrally managing and dynamically orchestrating multiple MCP servers/APIs into separate endpoints with flexible routing strategies. Prior to version 0.12.13, MCPB File Upload Handler extracts a ZIP file and reads manifest.json from it. The name field in the manifest is directly concatenated into a file path (line 107) without any sanitization or path traversal character validation. An attacker can craft a malicious MCPB file where manifest.name is set to something like ../../../etc/malicious, causing the file to be extracted to an arbitrary location on the file system. The cleanupOldMcpbServer function (line 110) also uses the unsanitized name, potentially allowing deletion of arbitrary directories. This issue has been patched in version 0.12.13.	N/A	More Details
CVE-2026-79749	MCPHub is a unified hub for centrally managing and dynamically orchestrating multiple MCP servers/APIs into separate endpoints with flexible routing strategies. Prior to version 1.0.32, MCPHub's SSRF guard in src/utils/ssrf.ts uses a custom isBlockedIpv6 function that only checks for loopback, link-local, unique-local, IPv4-mapped, and IPv4-compatible IPv6 addresses. IPv6 transition address families -- NAT64 (64:ff9b::/96), 6to4 (2002::/16), and Teredo (2001::/32) -- are not checked. An attacker who can specify a URL for an MCP server connection can encode a private IPv4 address inside one of these IPv6 forms to bypass the SSRF guard and reach internal infrastructure. This issue has been patched in version 1.0.32.	N/A	More Details
CVE-2026-80563	In the Linux kernel, the following vulnerability has been resolved: gpio: sloppy-logic-analyzer: fix use-after-free via debugfs trigger on unbind The "trigger" debugfs file has a hand-rolled ->write handler (trigger_write()) that dereferences the per-device gpio_la_poll_priv. The file is created with debugfs_create_file_unsafe(), and the handler never takes a debugfs reference. Nothing keeps the object alive while the handler runs. priv is allocated with devm_kzalloc(). devres frees it when the platform device is unbound. debugfs_create_file_unsafe() installs no full_proxy wrapper, so debugfs_remove_recursive() in gpio_la_poll_remove() does not wait for an in-flight trigger_write(). The blob_lock taken there does not help, because trigger_write() never takes it. A write that races an unbind therefore writes into freed memory: trigger_write() gpio_la_poll_remove() priv = m->private buf = memdup_user() [may sleep] mutex_lock(&priv->blob_lock) debugfs_remove_recursive() [no wait] mutex_unlock(&priv->blob_lock) (remove returns; devres frees priv) priv->trig_data = buf <-- use-after-free write priv->trig_len = count The race is reachable by root via /sys/bus/platform/drivers/gpio-sloppy-logic-analyzer/unbind. Create "trigger" with debugfs_create_file() instead. Its full_proxy wrapper makes debugfs_remove_recursive() drain any in-flight ->write before it returns. The use-after-free is confirmed under KASAN with a minimal reproducer of the same debugfs_create_file_unsafe() plus devm_kzalloc() pattern (available on request); it produces a	N/A	More Details

	slab-use-after-free write in the handler.		
CVE-2023-20511	Release of an invalid pointer in the AMD kernel mode driver (KMD) could allow a privileged attacker to create a double free condition potentially leading to arbitrary code execution.	N/A	More Details
CVE-2026-82481	The cohttp package before 6.3.0 for OCaml allows directory traversal.	N/A	More Details
CVE-2026-80573	In the Linux kernel, the following vulnerability has been resolved: Input: iforce - validate input packet lengths iforce_process_packet() reads fixed fields from joystick, wheel and status packets without first checking their lengths. In particular, the shared hats-and-buttons helper unconditionally reads data[6]. The status tail is a sequence of 16-bit effect addresses, but an incomplete final address is also consumed. A successful zero-length USB URB additionally reads the packet ID before the common parser is called. Reject the zero-length USB transfer, require the seven-byte joystick and wheel prefixes and the two-byte status prefix, and consume only complete status-tail addresses.	N/A	More Details
CVE-2026-80566	In the Linux kernel, the following vulnerability has been resolved: Input: hynitron_cstxxx - validate touch count and finger IDs The driver allocates max_touch_num input slots, which are indexed from zero through max_touch_num - 1. The current check allows a finger ID equal to max_touch_num to reach cst3xx_report_contact(). While the input core ignores out-of-range slot indices, reporting touch data without a valid slot change corrupts the touch state of the previously active slot. The touch count is read from the controller's report and is used to index the fixed-size report buffer without first checking its range. Reject counts larger than the supported number of touch slots before checking the trailing byte or parsing touch data. Reject finger IDs equal to or greater than max_touch_num, and return immediately when an invalid finger ID is encountered so that corrupt touch frames are discarded instead of reporting partial contact state. The V821 Avaota F1 board configures the vendor driver with one touch slot, so finger ID 1 is already invalid on that device.	N/A	More Details
CVE-2026-80567	In the Linux kernel, the following vulnerability has been resolved: Input: synaptics-rmi4 - propagate F54 worker errors to V4L2 queue Previously, rmi_f54_buffer_queue() waited for the worker thread to finish but ignored whether it succeeded. If the worker failed (e.g., due to a timeout or register read failure), the queue thread would silently return success, delivering stale or uninitialized memory to userspace. Add a 'report_error' field to struct f54_data to store the worker's exit status. Check this field in rmi_f54_buffer_queue() after the worker finishes, and mark the buffer as VB2_BUF_STATE_ERROR if an error occurred.	N/A	More Details
CVE-2026-51691	Incorrect access control in the setUploadSetting function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to manipulate the upload or flash workflow via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	N/A	More Details
CVE-2026-53507	oasdiff-action is a GitHub Action that detects breaking changes in OpenAPI specs and post a review on every pull request. Before version 0.0.51, the oasdiff actions resolved external $refs in the OpenAPI spec by default (allow-external-refs: true). When an action runs on a pull request whose spec is attacker-controlled — most importantly fork pull requests on public repositories — a $ref in that spec is fetched/read on the runner with no interaction required, enabling SSRF and disclosure of structured files on the runner. This issue has been patched in version 0.0.51.	N/A	More Details
CVE-2026-53508	oasdiff is a command-line and Go package that compares and detects breaking changes in OpenAPI specs. From version 1.13.2 through version 1.18.0, oasdiff did not enforce --allow-external-refs=false (library: openapi3.Loader.IsExternalRefsAllowed = false) when loading a spec from a git revision (the rev:path form, e.g. main:openapi.yaml). External $refs were resolved on that load path even when external refs were explicitly disabled, so the mitigation silently did not apply there. This issue has been patched in version 1.18.1.	N/A	More Details
CVE-2026-80571	In the Linux kernel, the following vulnerability has been resolved: powerpc/pseries: papr-phy-attest - validate cmd.length, plug mem leak In papr_phy_attest_create_handle(), the params->cmd.length is not validated before use, which can result in a buffer overlow. Check it and return -EINVAL if it is either 0 or exceeds sizeof(params->cmd). Also, params is freed on the success path but not error. Free it on errors after memory allocation. And free it on negative fd.	N/A	More Details
CVE-2026-9252	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-51692	Incorrect access control in the setWiFiGuestCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to establish or weaken guest wireless access via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	N/A	More Details
CVE-2026-18916	Any remote client can crash a NSD serve child, by throttling the TCP receive window after a TCP query. By continuously crashing the serve childs, the remote client can denial all TCP service to this NSD instance.	N/A	More Details
CVE-2026-51690	Incorrect access control in the setWanCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to alter upstream provisioning and connectivity via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	N/A	More Details

CVE-2026-64843	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-80223	Incorrect Authorization vulnerability in ash-project ash_graphql allows an authenticated subscriber in one tenant to receive another tenant's records over GraphQL subscriptions. The subscription resolver in AshGraphql.Graphql.Resolver authorizes each notification payload in memory: its fast path calls Ash.can/3 with run_queries?: false, which evaluates the read policy filter against the in-memory record via Ash.Expr.eval/2 and never issues a query. Ash applies multitenancy at query-build and data-layer-prefix time, not inside query.filter, so the evaluated policy carries no tenant condition and a tenant-B notification routed to a tenant-A subscriber is emitted whenever the policy filter is true. The single-notification clause has no tenant guard at all, and the batched clause checks only the head of the notification list, so non-head entries authorize purely in memory. A tenant-scoped read is reached only when filter evaluation fails. This issue affects ash_graphql: from 1.4.0 before 1.11.0.	N/A	More Details
CVE-2026-81633	Improper Input Validation vulnerability in ash-project ash_graphql allows an unauthenticated client to crash a relay node(id: ...) query with an unhandled KeyError. AshGraphql.Graphql.Resolver.resolve_node/2 decodes the client-supplied global ID with decode_relay_id/1, which only base64-decodes the string and splits it on : without validating the type segment. The decoded type is passed straight to Map.fetch! (type_to_domain_and_resource_map, type). Because fetch! raises on a missing key, a relay ID whose type segment is a valid atom that is not a relay-exposed type aborts the resolver before its resolve/2 clauses and their rescue handlers run, so the error never becomes a GraphQL error and may expose a stacktrace. Common resource names are easy to guess. The fix uses Map.fetch/2 and returns an Invalid node id error for unknown types. This issue affects ash_graphql: from 0.27.0 before 1.11.0.	N/A	More Details
CVE-2026-81636	Allocation of Resources Without Limits or Throttling vulnerability in ash-project ash_graphql allows an unauthenticated client to bypass the configured GraphQL query-complexity limit and force an unbounded database read. AshGraphql.Graphql.Resolver.query_complexity/3 multiplies child complexity by the requested page size only when the argument map contains :limit (offset pagination). Relay connections and keyset pagination use first and last, which never match that clause and fall through to the catch-all that returns child_complexity + 1. A nested relay query such as posts(first: 500) { edges { node { comments(first: 500) { ... } } } } therefore scores as trivially cheap while materializing the full fan-out, passing an Absinthe max_complexity cap that rejects the equivalent limit-based query. The fix adds first and last clauses clamped to the action's page size. This issue affects ash_graphql: from 0.16.23 before 1.11.0.	N/A	More Details
CVE-2026-81643	Incorrect Authorization vulnerability in ash-project ash_graphql delivers GraphQL subscription payloads for records a subscriber is not authorized to see. In AshGraphql.Subscription.Batcher, do_send/5 resolves the first notification of a batch and filters it with should_send?/1, which drops results whose errors are coded forbidden or not_found or carry no code, precisely so that unauthorized results are not disclosed. The remaining notifications in the batch are read from the process dictionary, re-run through the pipeline, and appended to the outgoing results without that filter. They reach pubsub.publish_subscription/2, and the not is_nil(record) guard drops only nil records, not error-carrying results. Any two qualifying notifications arriving within the default one-second batch interval suffice, and batching is the default path. The fix applies should_send?/1 to the whole batch. This issue affects ash_graphql: from 1.4.0 before 1.11.0.	N/A	More Details
CVE-2026-82367	Exposure of Data Element to Wrong Session vulnerability in ash-project ash_graphql can deliver one subscription's resolved records to a different subscriber's topic. AshGraphql.Subscription.Batcher.do_send/5 reads the resolved batch from the process dictionary via Process.get(:batch_resolved) and then unconditionally deletes it. That is sound only inside a task the library owns. On the :backpressure_sync and :noproc fallbacks do_send/5 runs inline in the publishing caller's process, so if a resolver inside an outer do_send/5 triggers another synchronous Ash notification, the inner call finds the outer run's value still under :batch_resolved, adopts it as its own result, and publishes it to the inner topic, a different subscription document with a different actor and tenant. It then deletes the key, so the outer run publishes nothing. The key is not namespaced by run, so records cannot be told apart. The fix saves, clears, and restores :batch_resolved around each run. This issue affects ash_graphql: from 1.4.0 before 1.11.0.	N/A	More Details
CVE-2026-56716	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-64839	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-64840	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-64841	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-64844	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-51689	Incorrect access control in the setUpgradeFW function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to trigger firmware-upgrade workflow changes via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	N/A	More Details

CVE-2026-80532	In the Linux kernel, the following vulnerability has been resolved: xfs: fix another iunlink infinite loop bug in online fsck xrep_iunlink_resolve_bucket is supposed to reconstruct as much of the incore prev and next unlinked list pointers based on what it finds on disk and in memory before we move on to relinking the truly lost inodes back into the unlinked list. However, it's still vulnerable to infinite loops that come in via the next_unlinked pointers. Fix this problem by remembering which inodes we've already seen and checking new agino pointers against that. If a bit is already set, either this is a loop or the inode has nonzero link count. We'll deal with the second case in a subsequent patch.	N/A	More Details
CVE-2026-19722	The WPvivid — Backup, Migration & Staging WordPress plugin before 0.9.133 does not validate the destination of files extracted from a backup package during restoration, allowing high privilege users such as administrators to write arbitrary files outside the intended restore directory, which can lead to code execution.	N/A	More Details
CVE-2026-77956	Improper Control of Generation of Code (Code Injection) vulnerability in ash-project ash_ai allows a remote, unauthenticated client to execute arbitrary Elixir code. AshAi.Actions.Prompt evaluates prompt content through EEx.eval_string/2. The documented prompt: fn input, context -> ... end form lets the prompt content be built from action arguments, so when a prompt action's text incorporates request data, that attacker-controlled text is compiled and run as an EEx template (Elixir source). Content such as <%= System.cmd(...) %> therefore executes on the server before any model request is made, requiring no authentication beyond reaching a prompt action. The fix stops evaluating function-supplied prompt content as EEx; only statically configured templates are evaluated. This issue affects ash_ai: from 0.1.0 before 1.0.0.	N/A	More Details
CVE-2026-81315	Origin Validation Error vulnerability in ash-project ash_ai allows a malicious web page to bypass the MCP server's DNS-rebinding protection and issue cross-site requests to a user's local MCP server with that user's actor. In AshAi.Mcp.Server, with the default allowed_origins: nil, origin_allowed?/3 accepts an origin when uri.host == conn.host and the forwarded scheme is https. Both values are attacker-controlled: conn.host comes from the Host header and the scheme is read from the raw x-forwarded-proto header with no trusted-proxy check. Under DNS rebinding the browser sends the attacker's origin and a matching host, and page JavaScript may set X-Forwarded-Proto: https, so the check passes with no TLS or proxy involved. The fix trusts only localhost origins by default; other origins require an explicit allowed_origins allowlist. This issue affects ash_ai: from 0.8.0 before 1.0.0.	N/A	More Details
CVE-2026-75760	Generation of Error Message Containing Sensitive Information vulnerability in ash-project ash_ai discloses provider request state and credentials in a user-facing validation error. In AshAi.Changes.Vectorize, when the embedding provider call fails the change added a changeset error whose message inspected the raw error term (An error occurred while generating embeddings: #{inspect(error)}). A plain-string add_error produces an Ash.Error.Changes.InvalidChanges in the :invalid class, which AshJsonApi and AshGraphql render back to the caller. The embedding client's error term is not sanitized, so it can carry the request URL, the provider response body, and, for HTTP clients that keep the request in the error struct, the outbound Authorization header with the provider API key. Failures are attacker-reachable via oversized or malformed vectorized content. The fix logs the raw error and returns a generic message. This issue affects ash_ai: from 0.1.0 before 1.0.0.	N/A	More Details
CVE-2026-80533	In the Linux kernel, the following vulnerability has been resolved: xfs: don't walk off the end of a null sc->sa.agi_bp in AGI repair LOLLM noticed a longstanding bug where xrep_iunlink_walk_ondisk_bucket tries to walk ragi->sc->sa.agi_bp to rebuild the unlinked inode lists. Unfortunately, it's possible for agi_bp to be null if the buffer verifier fails, so we have to use ragi->agi_bp (which skips verifier checks) instead.	N/A	More Details
CVE-2026-80534	In the Linux kernel, the following vulnerability has been resolved: xfs: fix ilock leak on error in xfs_dq_get_next_id xfs_dq_get_next_id() takes the quota inode ILOCK before calling xfs_iread_extents(). If xfs_iread_extents() fails, the function returns immediately without releasing the lock, leaking the quota inode ILOCK. This can leave the quota inode locked and cause subsequent quota operations to hang. Fix this by jumping to a common unlock path on error instead of returning directly.	N/A	More Details
CVE-2026-82564	Authorization Bypass Through User-Controlled Key vulnerability in ash-project ash_ai allows a caller of an identity-configured tool to update or destroy records it never identified, including every row in the table. In AshAi.Tool.Execution, identity_filter/3 built the update/destroy filter directly from the raw tool arguments as [{key, Map.get(arguments, to_string(key))}] and passed it to Ash.Query.do_filter/2. A map value is parsed as a predicate expression rather than a literal, so a caller can send {"public_ref": {"not_eq": "<own-ref>"}} and, combined with Ash.Query.limit(1) and Ash.bulk_update!/Ash.bulk_destroy!, retarget the write at a record it never identified; an omitted key yields an IS NULL filter that matches an arbitrary row. The fix casts each identity value to the field type, rejecting non-scalar inputs. This issue affects ash_ai: from 0.6.0 before 1.0.0.	N/A	More Details
CVE-2026-82579	Loop with Unreachable Exit Condition (Infinite Loop) vulnerability in ash-project ash_ai allows an attacker who can influence a model's output to hang the tool loop and drive unbounded, repeated model requests. AshAi.ToolLoop classifies a model response of :tool_calls, then filters the calls through normalize_tool_calls/2 and unprocessed_tool_calls/2. Both can empty the list: a call missing a valid name, or one reusing a tool_call_id that already has a result in history, is dropped. With an empty list the loop appended nothing and recursed with a byte-identical message list, so the conversation never advanced and the same request was re-sent every iteration. Under the supported max_iterations: :infinity this never terminated; otherwise it exhausted the full budget. Prompt-injected content can make the model re-emit a spent tool_call_id. The fix treats an empty post-filter list as terminal. This issue affects ash_ai: from 0.6.0 before 1.0.0.	N/A	More Details

CVE-2026-78693	Generation of Error Message Containing Sensitive Information vulnerability in ash-project ash_graphql allows a remote client to read internal field names that an application configured its error_handler to redact. In AshGraphql.Errors, each error is passed to the configured error_handler and the returned map is merged with the pre-handler path via Map.put_new(handled, :path, path). Because put_new defers to the handler only when the handler itself set :path, a sanitizing handler that returns a fresh map or deletes :path has that decision reverted. The re-injected path comes from build_error_path/5, which falls back to raw internal Ash attribute and argument names when no field_names mapping is configured. A validation failure on a non-exposed or nested field therefore returns internal names in the GraphQL error path, defeating the application's redaction. This issue affects ash_graphql: from 1.9.0 before 1.11.0.	N/A	More Details
CVE-2026-56715	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-56713	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-81322	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in ash-project ash_cloak allows anyone with access to logs, error trackers, or crash reports, or anyone who can trigger a validation error, to recover the plaintext of a field the library encrypts. AshCloak.Transformers.SetUpEncryption removes each cloaked attribute from the action's accept list and adds an action argument that carries the plaintext into the encryption change. That argument is built with sensitive?: attr.sensitive?, inheriting the flag from the source attribute, so a cloaked attribute declared without sensitive? true produces a non-sensitive argument. It is the only place the cleartext value lives, and the one place Ash will not redact: it appears verbatim in inspect(changeset), Ash.Error.Invalid and validation error messages, telemetry, :sys dumps, and error-tracker payloads. The generated encrypted attribute and decrypt calculation are already hardcoded sensitive. This issue affects ash_cloak: from 0.1.0 before 0.4.0.	N/A	More Details
CVE-2026-74749	In the Linux kernel, the following vulnerability has been resolved: rseq: Prevent hard lockup on granted time slice extension __exit_to_user_mode_loop() invokes rseq_grant_timeslice_extension() with interrupts enabled. If the extension is granted it invokes hrtimer_rearm_deferred_tif() to ensure that a pending deferred hrtimer rearm is handled before exiting to user space. Though this invokes __hrtimer_rearm_deferred() which expects to be invoked with interrupts disabled as it takes hrtimer_cpu_base::lock with raw_spin_lock(). That's a livelock waiting to happen and caught by lockdep: WARNING: ./include/linux/hrtimer_rearm.h:17 at irqentry_exit, CPU#1: slice_test WARNING: inconsistent lock state inconsistent {IN-HARDIRQ-W} -> {HARDIRQ-ON-W} usage. Prevent this by disabling interrupts around the invocation of hrtimer_rearm_deferred_tif() in rseq_grant_timeslice_extension(). [tglx: Massaged change log]	N/A	More Details
CVE-2026-80524	In the Linux kernel, the following vulnerability has been resolved: optee: ffa: Add NULL check in optee_ffa_lend_protmem Sashiko (locally) reports a possible null dereference under memory pressure due to the lack of validation of the allocated pointer. Fix that by adding the missing check.	N/A	More Details
CVE-2026-80525	In the Linux kernel, the following vulnerability has been resolved: ASoC: SOF: ipc4-topology: Refresh copier IPC payload before widget setup The ipc_config_data buffer for copier widgets is built once during ipc_prepare (called from sof_pcm_setup_connected_widgets) and cached for reuse. For host copiers this buffer contains the copier_data with gtw_cfg.node_id (host DMA ID). For DAI copiers it additionally includes a dma_config_tlv trailer with stream_id and dma_channel_id for HDA link DMA. On suspend/resume, both host and link DMA streams are released and re-allocated with potentially different stream tags. The underlying copier_data and dma_config_tlv structures are correctly updated by host_config and sdw_hda_dai_hw_params respectively. However, since the widget list (spcm->stream[].list) persists across suspend, sof_pcm_hw_params skips sof_pcm_setup_connected_widgets and ipc_prepare never runs again to rebuild ipc_config_data. The stale cached payload is then sent to firmware with boot-time DMA channel assignments, causing DMA channel conflicts that lead to firmware errors and crashes. Fix this by refreshing copier_data and dma_config_tlv portions of ipc_config_data in sof_ipc4_widget_setup right before the IPC message is sent. This ensures the payload always reflects the current DMA state regardless of whether ipc_prepare ran. For DAI copiers, the gtw_cfg.config_length in copier_data is temporarily inflated to include the TLV size (matching the ipc_config_data layout) before copying, then restored, mirroring what sof_ipc4_prepare_copier_module does when first building the buffer.	N/A	More Details
CVE-2026-80529	In the Linux kernel, the following vulnerability has been resolved: xfs: don't swallow dquot recovery verification errors xlog_recover_dquot_commit_pass2() validates the recovered dquot with xfs_dqblk_verify() and, on failure, sets error = -EFSCORRUPTED and jumps to out_release. But out_release unconditionally returns 0, so the corruption error is discarded: the caller xlog_recover_items_pass2() sees success, log recovery proceeds as if the dquot were valid, and the corrupt quota buffer can be written back to disk.	N/A	More Details
CVE-2026-81318	Incorrect Authorization vulnerability in ash-project ash_sql allows a caller in a schema-based multitenant application to receive aggregate values computed from another tenant's rows. When an aggregate is computed over a distinct query, AshSql.AggregateQuery.add_single_aggs/5 rebuilds the outer query from query.from.source alone, which is only the {table, schema} tuple and does not carry query.prefix or query.from.prefix. For strategy(:context) multitenancy those hold the tenant schema, so the rebuilt outer query reads the repo's default schema while the inner correlated subquery still reads the tenant schema, and the two are joined only on primary key. The aggregate, and any relationship join added off the prefix-less binding, is then computed against the wrong tenant's rows. The neighbouring limit and exists branches instead wrap the query with subquery/1, which preserves the prefix. This issue affects ash_sql: from 0.1.0	N/A	More Details

	before 0.7.1.		
CVE-2026-81316	Incorrect Authorization vulnerability in ash-project ash_sql allows a caller to receive an aggregate value computed over rows a more restrictive filter should have excluded, disclosing counts, sums, or lists across an authorization or tenancy boundary. AshSql.Aggregate.different_queries?/2 reports two aggregate queries as different only when their filter and their sort both differ. Aggregate queries rarely carry a sort, so two aggregates that share a name but carry entirely different filters compare as identical. The colliding aggregate keeps its name and is treated as already computed, and select_aggregates returns the first-registered variant's value. The same name reaches the builder twice with different filters when actor or tenant context is stamped into each aggregate's query, so a narrowly filtered aggregate can be served the value of a previously registered broad one. This issue affects ash_sql: from 0.1.0 before 0.7.1.	N/A	More Details
CVE-2026-80227	Incorrect Comparison vulnerability in ash-project ash_sql allows a user to pad a string field with tab, newline, carriage-return, or form-feed characters and pass a trimmed uniqueness or equality check in the database that the same expression would fail in memory (or the reverse). string_trim/1 compiles to REGEXP_REPLACE patterns built from an Elixir string in which \s is the escape for a single space (codepoint 32), not a regex whitespace class. The generated SQL therefore removes only literal spaces and leaves tabs, newlines, carriage returns, and form feeds in place, whereas String.trim/1 in Elixir removes them all. Any Ash filter, validation, or identity that relies on string_trim/1 then behaves differently depending on whether Ash pushes the expression down to SQL or evaluates it in memory, so padded input can register a near-duplicate value or slip past a trimmed comparison. This issue affects ash_sql: from 0.1.0 before 0.7.1.	N/A	More Details
CVE-2026-78691	Improper Neutralization of Special Elements in Data Query Logic vulnerability in ash-project ash_sql allows a user who supplies a search term to contains/2, string_starts_with/2, or string_ends_with/2 to inject live SQL LIKE wildcards, turning a literal substring search into an attacker-controlled pattern match. The escape helpers in AshSql.Expr prefix % and _ with a backslash but never escape a backslash already present in the input. Because backslash is the default LIKE escape character, the escaping defeats itself: the input \% becomes the pattern fragment \\%, where \\ is a literal backslash and the attacker's % remains a live wildcard. The search value stays parameterized, so this is confined to the LIKE pattern grammar rather than full SQL. An attacker can widen matches to probe values, slip past a negated contains(...) guard, or crash the query with a trailing lone backslash. This issue affects ash_sql: from 0.1.1-rc.10 before 0.7.1.	N/A	More Details
CVE-2026-78228	Uncontrolled Recursion vulnerability in ash-project ash_oban allows a user who can drive a trigger's on_error action to fail on the final attempt to exhaust worker CPU and memory, denying service. The generated worker's atomic handle_error/4 runs the trigger's on_error action on a job's final attempt inside a rescue that, when the action itself raises, calls handle_error/4 again with the same job. The job's attempt still equals max_attempts, so it re-enters the same clause and re-runs the failing action, with no exit. Any deterministic on_error failure (a data-layer outage, a misconfigured action, or a record the action rejects) loops forever; because the recursive call is not in tail position, each iteration retains a formatted stacktrace and the process heap grows without bound while the failing statement is re-issued against the data layer until the runtime kills the worker. This issue affects ash_oban: from 0.8.0-rc.1 before 0.8.14.	N/A	More Details
CVE-2026-78038	Improperly Controlled Modification of Dynamically-Determined Object Attributes vulnerability in ash-project ash_oban allows a user whose input reaches the :args option of AshOban.build_trigger/3 to retarget an update or destroy trigger at another record, including across tenants. build_trigger/3 builds the trusted job arguments with atom keys (:primary_key, :tenant, :action_arguments) and merges the caller's :args underneath so the trusted values win on collision. Because Oban job arguments round-trip through JSON, the caller's keys arrive as strings, so Map.merge sees no collision and both keys survive. When the job is persisted the JSON object is de-duplicated keeping the last (string) key, and the worker reads the caller's value. The documentation describes :args as unable to affect the action, so an application that forwards user input into it for uniqueness scoping is exposed to authorization bypass and tenant isolation breaks. This issue affects ash_oban: from 0.2.5 before 0.8.14.	N/A	More Details
CVE-2026-77454	Incorrect Authorization vulnerability in ash-project ash_sql allows a caller to bypass a scoping or authorization filter expressed as exists/2 over a relationship that declares both a limit (or from_many?) and a parent(...)-referencing filter or sort. AshSql.Join.related_query/3 skips the caller-supplied exists predicate for such relationships and delegates it to limit_from_many/5. When the relationship's own filter or sort references parent(...), limit_from_many/5 takes a branch that drops both the limit and the predicate, emitting a bare correlated EXISTS with no predicate. The check then matches any record that has any related row. Most severely, when the expression backs a policy (for example authorize_if expr(exists(memberships, user_id == ^actor(:id)))), the actor-scoping condition disappears and the policy passes for any actor with any related row. This issue affects ash_sql: from 0.4.1 before 0.7.1.	N/A	More Details
CVE-2026-74740	In the Linux kernel, the following vulnerability has been resolved: net/sched: act_api: fix TOCTOU NULL deref on a->goto_chain tcf_action_exec() handles TC_ACT_GOTO_CHAIN by first checking rcu_access_pointer(a->goto_chain) and then calling tcf_action_goto_chain_exec(), which does a second, independent rcu_dereference_bh(a->goto_chain) read and immediately dereferences chain->filter_chain. A concurrent tcf_action_set_ctrlact() (e.g. the gact replace path) can clear a->goto_chain between the two reads, so the second read returns NULL and tcf_action_goto_chain_exec() dereferences NULL. Fix the race by doing a single rcu_dereference_bh() read of a->goto_chain in tcf_action_exec(), checking it once for NULL, and passing the resulting chain pointer into tcf_action_goto_chain_exec(). This turns the split check/use into a single check/use on one value.	N/A	More Details

CVE-2026-74738	In the Linux kernel, the following vulnerability has been resolved: regmap: sdw-mbq: don't call an unset readable_reg callback regmap_sdw_mbq_poll_busy() decides whether to poll the Function Busy bit by calling ctx->readable_reg(), which is a straight copy of config->readable_reg. That callback is optional: regmap_readable() treats a NULL ->readable_reg as "every register is readable", and drivers rely on that. es9356 and tac5xx2-sdw both build an MBQ regmap without one. Since commit ca1b11b36d82 ("regmap: sdw-mbq: Allow defers on undeferrable controls") the poll runs on every -ENODATA, not only for Controls the driver marked deferrable, so any of those devices answering COMMAND_IGNORED takes the kernel through a NULL function pointer. Treat a missing callback the way the rest of regmap does and poll.	N/A	More Details
CVE-2026-74735	In the Linux kernel, the following vulnerability has been resolved: l2tp: fix tunnel and session refcount leak on seq_file release In pppol2tp_proc_open() and l2tp_dfs_seq_open(), iteration state (pd->tunnel and pd->session) is kept in seq_file private data to allow iteration across multiple read() system calls. However, if userspace closes /proc/net/pppol2tp or /sys/kernel/debug/l2tp/tunnels before reading to end-of-file (EOF), any tunnel or session reference stored in pd->tunnel / pd->session is left un-dropped when seq_file private data is freed. Fix this by dropping any remaining pd->tunnel and pd->session references in pppol2tp_proc_release() and l2tp_dfs_seq_release() when closing the file.	N/A	More Details
CVE-2026-82649	SiYuan Windows installer before version 3.8.1 (affected versions >= 2.0.14) contains an uncontrolled search path element vulnerability in its NSIS installer, which invokes system executables such as TASKKILL by name rather than by absolute path. Because NSIS nsExec::Exec resolves these calls using a search path that includes the installer's own launch directory ahead of System32, an attacker who plants a malicious executable (e.g., a renamed TASKKILL.exe) in that directory can have it executed when the installer runs. These calls occur in electron-builder's preInit hook before the license page is displayed, and with an all-users (elevated) install the planted binary executes with an elevated token, resulting in local privilege escalation.	N/A	More Details
CVE-2026-74734	In the Linux kernel, the following vulnerability has been resolved: firewire: ohci: fix NULL pointer dereference in ar_context_release During the error handling path of the driver's probe function, a NULL pointer dereference can occur in ar_context_release(). When pci_probe() fails early (e.g., if pcim_enable_device() or MMIO mapping fails), the devres cleanup mechanism invokes release_ohci(). This function unconditionally calls ar_context_release() to clean up the asynchronous receive contexts. However, if ar_context_init() was not yet called, ctx->ohci remains NULL (as the fw_ohci structure is zero-initialized by devres_alloc()). ar_context_release() immediately dereferences ctx->ohci to get the dev pointer before checking if the context was actually initialized, leading to a crash: Oops: general protection fault, probably for non-canonical address 0xdffffc0000000001: 0000 [#1] SMP KASAN NOPTI KASAN: null-ptr-deref in range [0x0000000000000008-0x000000000000000f] RIP: 0010:ar_context_release+0x3f/0x380 drivers/firewire/ohci.c:543 Call Trace: release_ohci+0x3f/0x60 drivers/firewire/ohci.c:3567 release_nodes drivers/base/devres.c:546 [inline] devres_release_all+0x1a8/0x260 drivers/base/devres.c:576 device_unbind_cleanup drivers/base/dd.c:597 [inline] really_probe+0x451/0xae0 drivers/base/dd.c:772 To fix this, move the assignment of the dev pointer after the !ctx->buffer check. If ctx->buffer is NULL, it indicates that the context was never successfully initialized and there is nothing to release, safely avoiding the dereference of the uninitialized ctx->ohci pointer.	N/A	More Details
CVE-2026-54556	Http4s is a Scala interface for HTTP services. Prior to 0.23.35 and 1.0.0-M47, an unauthenticated HTTP/2 peer can cause an out-of-memory denial of service in the Ember backend with HTTP/2 enabled. The Hpack wrapper in ember-core/shared/src/main/scala/org/http4s/ember/core/h2/Hpack.scala concatenates HEADERS and CONTINUATION frame fragments and decodes them into a single List, but maxHeaderSize accounting does not include indexed headers or HPACK per-header overhead. A small compressed header block can therefore expand into a much larger decoded representation that remains in memory for processing. Servers exposed to untrusted HTTP/2 traffic and clients directed to an untrusted HTTP/2 server are affected, and concurrent malicious connections can exhaust the process heap. This issue is fixed in versions 0.23.35 and 1.0.0-M47.	N/A	More Details
CVE-2026-78699	Unchecked Return Value vulnerability in ash-project ash_postgres allows a user who can drive a tenant rename to a name that collides with an existing tenant's schema to have their tenant record repointed at that other tenant's live schema, gaining access to its data. AshPostgres.MultiTenancy.rename_tenant/3 issues the ALTER SCHEMA ... RENAME TO ... with the non-raising Ecto.Adapters.SQL.query/2, discards its {:ok, _} | {:error, _} result, and unconditionally returns :ok. PostgreSQL rejects the rename when the target schema already exists (and on insufficient privilege or lock timeout), but that failure never reaches the caller. The calling manage_tenant update action therefore sees success and commits the tenant row with the new name, which is the schema of a different existing tenant, so subsequent reads and writes for that tenant run against the other tenant's data. This issue affects ash_postgres: from 0.25.0 before 2.13.0.	N/A	More Details
CVE-2026-81319	Deserialization of Untrusted Data vulnerability in ash-project ash_cloak allows an attacker who can influence the bytes of an encrypted column to crash the BEAM node, by triggering unbounded atom creation or a decompression bomb during decryption. AshCloak.Calculations.Decrypt decodes the decrypted binary with Ash.Helpers.non_executable_binary_to_term/1 without the :safe option, so atoms in the payload are interned during the decode and never garbage collected, and the term format's compressed form is inflated transparently. vault.decrypt!() is the only barrier and stops tampering only for an authenticated cipher. Cloak also ships the unauthenticated AES.CTR, whose ciphertext an attacker who knows their own plaintext can XOR into any same-length payload without the key, so an ordinary read of the forged column reaches the decoder. A few hundred kilobytes of distinct atoms exhausts the atom table, or a small compressed payload inflates to gigabytes. This issue affects ash_cloak: from 0.1.0 before 0.4.0.	N/A	More Details

CVE-2026-82580	Generation of Error Message Containing Sensitive Information vulnerability in ash-project ash_ai discloses internal error text to chat users. In AshAi.ToolLoop and AshAi.Tools, an exception raised while executing a tool was serialized verbatim with Exception.message/1 into the tool-result content. That content is appended to the conversation, emitted as a {:tool_result, ...} stream event, and sent back to the model, which typically relays it to the user. No filtering happened first, so anything raised inside a tool callback or lifecycle hook (database constraint messages, adapter errors, query fragments, policy or validation internals) was echoed as-is. A chat user who can steer tool arguments into a raising code path receives the raw internal text. The fix routes raised tool errors through the same safe formatter used for other tool errors. This issue affects ash_ai: from 0.6.0 before 1.0.0.	N/A	More Details
CVE-2026-75757	Reliance on Cookies without Validation and Integrity Checking vulnerability in ash-project ash_admin lets an attacker who controls a sibling subdomain rebind an admin's session to a different actor, tenant, or authorization mode. AshAdmin's client JavaScript read its state cookies (tenant, actor_resource, actor_primary_key, actor_action, actor_domain, actor_authorizing, actor_paused) by matching the cookie name with an unanchored regular expression (new RegExp(name + "=([^;]+)")) against the whole document.cookie. Any cookie whose name merely ends with the requested name therefore matches, and whichever is serialized first wins. Because cookies are shared across a registrable domain, a compromised sibling subdomain can set a shadowing cookie (for example xactor_authorizing) with Domain=.example.com that flows unvalidated into the admin's LiveSocket connect params. The fix matches cookie names by exact equality. This issue affects ash_admin: from 0.9.1 before 1.3.1.	N/A	More Details
CVE-2026-77850	Stored Cross-site Scripting vulnerability in ash-project ash_admin executes attacker-supplied record content as script in an administrator's browser. The relationship typeahead components AshAdmin.Components.Resource.RelationshipField and AshAdmin.Components.Resource.ManagedRelationshipSelectField highlight the matched search term by wrapping it in <b> tags and rendering the whole string with Phoenix.HTML.raw/1. The highlighted value is the destination record's label_field, ordinary database content that is often written by lower-privileged users. Because raw/1 disables output escaping for the entire string, a stored label such as <img src=x onerror=...> runs as JavaScript in the admin's session as soon as a matching record appears in the dropdown, giving the attacker the admin's privileges over everything AshAdmin exposes. The fix HTML-escapes the label before inserting the highlight markup. This issue affects ash_admin: from 0.13.0 before 1.3.1.	N/A	More Details
CVE-2026-80539	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: disallow multiple FENCE chunks in one submit amdgpu_cs_pass1() dispatches on chunk_id once per chunk without rejecting repeated ids. p->uf_bo is a single-slot field, so a submission carrying two AMDGPU_CHUNK_ID_FENCE chunks runs amdgpu_cs_p1_user_fence() twice, and the second run overwrites p->uf_bo with a freshly referenced BO without dropping the reference taken by the first. amdgpu_cs_parser_fini() only unrefs the final p->uf_bo, so every FENCE chunk but the last leaks a BO reference. The leaked BO outlives handle close and process exit. Reject duplicate FENCE chunks the same way commit fec5f8e8c6bc ("drm/amdgpu: disallow multiple BO_HANDLES chunks in one submit") did for p->bo_list. (cherry picked from commit 665b1fc2a1845206408f9a2c6da67101789edb82)	N/A	More Details
CVE-2026-80543	In the Linux kernel, the following vulnerability has been resolved: s390/zcrypt: Pad trailing CCA or EP11 message with zeros The both functions xcrb_msg_to_type6cprb_msgx() and xcrb_msg_to_type6_ep11cprb_msgx() copy the user space message into a kernel buffer based on the message length. But on further processing the message is supposed to be 4 byte length adjusted. Thus up to 3 bytes of uninitialized kernel memory are forwarded to further processing steps and may unwanted expose kernel memory to the crypto card firmware. This patch contains code to pad the gap between user space copied message and message buffer length sent down to further processing of the CCA or EP11 message to zeros.	N/A	More Details
CVE-2026-19538	The BLOCKED access control list items that are evaluated to deny access on the the proxy protocol port can be bypassed completely when connecting over TCP or TLS and sending the query twice on connection that is kept open.	N/A	More Details
CVE-2026-19401	Any remote client can crash a (debugging/non-release build type) NSD serve child by sending it a special crafted message with a specially tuned number of DNS Cookie options (17 when UDP payload size is 512). By continuously crashing the serve childs, the remote client can severely hamper or, when positioned sufficiently close, deny all DNS service.	N/A	More Details
CVE-2026-74754	In the Linux kernel, the following vulnerability has been resolved: scsi: core: pair EH runtime PM get and put shost->eh_noresume is currently consulted twice in one error handling iteration: once before scsi_autopm_get_host() and once again before scsi_autopm_put_host(). That is racy when a PM-triggered error path flips shost->eh_noresume while the SCSI EH thread is still running. The problem flow looks like this: PM path ufshcd_set_dev_pwr_mode() shost->eh_noresume = 1 ufshcd_execute_start_stop <-- trigger EH ... shost->eh_noresume = 0 EH path scsi_error_handler() if (!shost->eh_noresume) scsi_autopm_get_host() <-- skipped ... if (!shost->eh_noresume) scsi_autopm_put_host() <-- executed later In that case one EH iteration can skip autoresume on entry and still drop a runtime PM reference on exit. That leaves an unmatched runtime PM put and can trigger a runtime PM usage count underflow. Fix this by making eh_noresume a regular bool so it can be accessed with READ_ONCE() and WRITE_ONCE(). Snapshot it once per EH iteration and use that snapshot for both runtime PM get and put decisions.	N/A	More Details
	When ranges are used for access control (i.e. of the form 1.2.3.4-1.2.3.25), because NSD wrongly compares the IP address with the range on little endian systems, IPs that were meant to be allowed may be denied,		

CVE-2026-18664	and, IPs that were meant to be denied access could be allowed. An IPv4 address is compared with IPv4 ranges as unsigned 32 bit numbers directly with the endianness of the host, but the values to compare are in network byte order (big-endian). With IPv6 addresses the comparison is done in 4 times a unsigned 32 bit number comparison, again with the endianness of the host where all values are actually in network bye order.	N/A	More Details
CVE-2026-58108	The personal access token removal query selects from PersonalAccessTokenDB but filters on columns of Session, with no join between them. SQLAlchemy resolves that as an implicit cross join, so the filter does not constrain the delete to the calling user's own token in the way the code reads as intending. This way a user can delete all personal access tokens in the system.	N/A	More Details
CVE-2026-15366	A control logic defect in a specific built-in webpage of Kids Mode allows users to view local gallery photos directly within the page	N/A	More Details
CVE-2026-15365	A pop-up logic flaw in a certain feature of Kids Mode allows users to bypass password verification and use Quick Apps outside the app.	N/A	More Details
CVE-2026-77790	The RegistrationMagic WordPress plugin before 6.0.9.4 does not sanitise and escape a parameter before using it in a SQL statement, which could allow high privilege users such as admin to perform SQL injection attacks.	N/A	More Details
CVE-2026-78074	Joomla Extension - miniorgange.com - Unauthenticated arbitrary extension deinstallation via various miniOrange extensions - a missing authentication check allows unauthenticated actors to delete arbitrary installed extensions. Only the free versions of the miniOrange plugins are affected.	N/A	More Details
CVE-2026-78075	Joomla Extension - joomshaper.com - Broken Object-Level Authorization in Blog Image Deletion in Helix Ultimate < 2.2.10 - `Blog::remove_image()` checked whether the user was authorized to edit the article ID passed in the request, but did not verify whether the specified image path (src) belonged to that article. On Joomla 3 builds where physical file deletion was triggered, an author could supply their own article ID alongside an arbitrary file path under the `/images/` directory to delete arbitrary files.	N/A	More Details
CVE-2026-78076	Joomla Extension - joomshaper.com - Broken Access Control & Missing Authorization in MegaMenu Settings in Helix Ultimate < 2.2.10 - The AJAX endpoint save-megamenu-settings failed to enforce item-level and menu-level edit permissions (core.edit on com_menus.item.{id} or core.admin). An authenticated user could submit modified layout parameters for arbitrary menu items without proper authorization.	N/A	More Details
CVE-2026-78077	Joomla Extension - joomshaper.com - Stored Cross-Site Scripting (XSS) in MegaMenu Layout Container & Embed Inputs in Helix Ultimate < 2.2.10 - Unsanitized column and item configuration values stored within the MegaMenu layout JSON were rendered without complete contextual escaping, allowing injection of malicious HTML/JS. Stricter sanitization and tag allowlists via `InputFilter` and `htmlspecialchars` were implemented.	N/A	More Details
CVE-2026-78078	Joomla Extension - joomshaper.com - Privileged File Upload Bypass via Content Spoofing in Helix Ultimate < 2.2.10 - Image uploads previously validated only file extension and basic size parameters. Non-image files disguised with raster extensions could be uploaded. Added strict MIME verification and GD binary raster decoding (imagecreatefromstring) to reject invalid/malformed images fail-closed.	N/A	More Details
CVE-2026-78079	Joomla Extension - joomshaper.com - Open Redirect via Base64 Return Parameter in Helix Ultimate < 2.2.10 - Return redirect parameters accepted arbitrary Base64 strings without verifying whether the resolved target was an internal site URL via Uri::isInternal.	N/A	More Details
CVE-2026-51684	Incorrect access control in the setStorageCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to alter the storage-related service state via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	N/A	More Details
CVE-2026-51686	Incorrect access control in the setWiFiEasyCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to reconfigure or disable wireless networks via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	N/A	More Details
CVE-2026-51687	Incorrect access control in the setWiFiEasyGuestCf function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to create or weaken guest wireless access via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	N/A	More Details
CVE-2026-51688	Incorrect access control in the setWiFiSignalCfg function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to reduce wireless power or cause a Denial of Service (DoS) via sending a crafted POST request to /cgi-bin/cstecgi.cgi.	N/A	More Details
CVE-2026-80542	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix NULL pointer dereference in amdgpu_dm_crtc_set_vblank() amdgpu_dm_crtc_set_vblank() dereferences acrtc_state->stream when vblank is enabled/queried from DRM_IOCTL_MODE_CRTC_GET_SEQUENCE before a stream is attached to it. BUG: kernel NULL pointer dereference, address: 0000000000000008 RIP: amdgpu_dm_crtc_set_vblank+0x6b/0x4d0 [amdgpu] Call Trace: drm_vblank_enable drm_vblank_get drm_crtc_get_sequence_ioctl drm_ioctl_kernel drm_ioctl Reproduced by running VKCTS with WSI tests enabled on RADV. Guard the enable path on acrtc_state->stream being non-NULL, matching the existing checks in this function. (cherry picked from commit 7b1b31bf6942e6f43509b48da23f8e27269aac39)	N/A	More Details

CVE-2026-19410	An Incorrect Authorization vulnerability in GitHub Trigger Comment Control in Google Cloud Build prior to 2026-06-24 on Google Cloud Platform allows a remote attacker to execute unreviewed code in the build environment using webhook suppression. This vulnerability was patched on 24 June 2026, and no customer action is needed.	N/A	More Details
CVE-2026-81852	Use of Insufficiently Random Values vulnerability in ash-project ash_admin ships a hardcoded, publicly known CSP nonce, defeating nonce-based Content-Security-Policy protection. When mounted without :csp_nonce_assign_key, AshAdmin.Router.ash_admin/2 defaulted the img, style, and script nonces to the literal constant ash_admin-Ed55GFnX, which AshAdmin.Layouts wrote verbatim into the nonce attribute of its inline <style> and <script> tags on every response. The value is a compile-time constant published in the repository and is never rotated per request. If an application's CSP script-src allow-lists that documented default, any HTML-injection sink on an admin page can reuse the known nonce to run inline scripts the policy was meant to block. The fix generates a fresh random nonce per request. This issue affects ash_admin: from 0.10.8 before 1.3.1.	N/A	More Details
CVE-2026-82838	The default docker image shipped for Venueless did not properly ensure that uploaded SVG files could not be delivered with executable JavaScript content. A valid Content Security Policy is now set.	N/A	More Details
CVE-2026-81853	Authorization Bypass Through User-Controlled Key vulnerability in ash-project ash_admin turns a record-lookup URL into an equality oracle over sensitive attributes. AshAdmin.Helpers.decode_primary_key/2 decodes the composite-primary-key form (Base64 plus ETF) and returns the decoded map verbatim as the lookup filter, without checking that its keys are the resource's primary-key fields. The deserialization guards bound size, block new atoms and funs, and reject nested expressions, but none restricts which fields come back, and :safe still allows any already-interned attribute name. An attacker can therefore encode %{api_token: "guess"} and have it spliced into the lookup filter, brute-forcing a sensitive attribute value (API token, reset token) one equality guess at a time; Map.to_list/1 also accepts structs, yielding a bogus __struct__ key. The fix rejects any decoded key that is not a real primary-key field. This issue affects ash_admin: from 0.1.0 before 1.3.1.	N/A	More Details
CVE-2026-82673	Improper Limitation of a Pathname to a Restricted Directory (Path Traversal) vulnerability in ash-project ash_admin allows writing attacker-controlled bytes to arbitrary paths on the server. AshAdmin.Components.Resource.Form.consume_file_uploads/1 builds the destination as Path.join([tmp_dir, entry.client_name]) and writes it with File.cp!/2. entry.client_name is the browser-supplied filename and is not sanitized, and Path.join/1 does not normalize ... An upload named ../../../../var/www/app/priv/static/x.png therefore escapes the random temp directory and lands anywhere the BEAM user can write, enabling arbitrary file write and potentially remote code execution by overwriting application assets, configuration, or cron/ssh files. The only guard is an extension allowlist defaulting to :any that checks only the extension. The fix strips path components with Path.basename/1 before joining. This issue affects ash_admin: from 0.13.7 before 1.3.1.	N/A	More Details
CVE-2026-82681	Improper Encoding or Escaping of Output vulnerability in ash-project ash_admin lets an attacker who controls a record's string primary key rewrite the target of AshAdmin's row-action links. The Table, DataTable, and Show components built row-action URLs by raw string interpolation, splicing the primary key (and table, domain, and resource names) into the query string without URL-encoding. Ash resources routinely use user-settable string primary keys (slugs, emails). Because Plug.Conn.Query resolves duplicate parameters last-wins and primary_key is interpolated last, a stored key such as foo&action_type=destroy injects parameters that override the link, so an admin clicking edit is sent to a destroy form or an arbitrary resource; a # truncates the query into a fragment. The fix builds every link with URI.encode_query/1, encoding all interpolated values. This issue affects ash_admin: from 0.3.0-rc.0 before 1.3.1.	N/A	More Details
CVE-2026-82722	Allocation of Resources Without Limits or Throttling vulnerability in ash-project ash_admin lets any client that can reach the admin LiveView exhaust the BEAM atom table and crash the entire node. Two LiveView event handlers interned atoms from unvalidated client input: AshAdmin.PageLive's set_actor built modules from the resource/domain payload with Module.concat/1, and AshAdmin.Components.Resource.Show's calculate converted every submitted form key with String.to_atom/1. Atoms are never garbage collected and the table is capped, so flooding either event with random names mints a new atom per request until the VM aborts, taking down every application on the node. The fix resolves the submitted resource/domain against the known shown resources and maps calculation keys to declared arguments, so no client-supplied string is interned. This issue affects ash_admin: from 0.1.0 before 1.3.1.	N/A	More Details
CVE-2026-80535	In the Linux kernel, the following vulnerability has been resolved: xfs: don't double-lock when deleting a self-referential directory LOLLM notices that the dirtree scrubber can detect a directory that refers to itself. In this case, it's not correct for the directory tree repair code to try to iolock/ilock both sc->ip and dp, because they're the same inode. Fix this by detecting that corner case and handling it appropriately.	N/A	More Details
CVE-2026-77846	Improper Neutralization of Special Elements in Data Query Logic vulnerability in ash-project ash_sqlite allows an attacker who controls a get_path/2 segment to traverse into nested JSON the application never exposed, disclosing private or sensitive? embedded fields. AshSqlite.SqlImplementation builds the SQLite json_extract path with "$." <> Enum.join(right, "."), so a single segment containing ., [,], or $ re-interprets the JSON path (for example "private.secret" descends two levels instead of naming one key). The path is bound as a parameter, so this is confined to the JSON-path grammar rather than SQL. Any endpoint that lets user input reach a get_path segment (a common pick-a-field pattern) can read nested values it never meant to expose. This issue affects ash_sqlite: from 0.1.2-rc.0 before 0.2.18.	N/A	More Details

CVE-2026-75759	Improper Verification of Cryptographic Signature vulnerability in erlef oidcc allows an unauthenticated attacker to impersonate an arbitrary user via an encrypted ID token or JARM response carrying no nested signature. OpenID Connect Core 1.0 section 2 requires that an encrypted ID token be signed then encrypted, with the result being a Nested JWT, and JARM processing rule 5 requires the client to check the signature unconditionally. oidcc instead accepted a JWE wrapping unsigned claims as fully validated, so anyone holding the relying party's public encryption key could mint a token with an arbitrary sub, iss, and aud without possessing the provider's signing key. In oidcc_jwt_util:verify_decrypted_token/4, a decrypted payload that is not a signed JWS fell back to parsing the plaintext claims and returning them with no verifying key. oidcc_token:int_validate_jwt/4 then matched on the JOSE structure type rather than on whether a signature had been verified, and returned success. The JARM path in oidcc_token:validate_jarm/3 is reachable through the browser front channel. UserInfo responses are not affected, because OpenID Connect Core 1.0 section 5.3.2 permits them to be encrypted without also being signed. This issue affects oidcc: from 3.2.0-beta.1 before 3.9.0.	N/A	More Details
CVE-2026-77970	Cleartext Storage of Sensitive Information vulnerability in ash-project ash_paper_trail allows an attacker with read access to the generated version resource to recover sensitive values nested inside embedded resources, unions, or lists. sensitive_attributes :redact and :ignore only act on the tracked resource's top-level attributes. maybe_redact_changes/3 and the stored-action-input path in AshPaperTrail.Resource.Changes.CreateNewVersion derive the sensitive set from the resource's own attributes and never descend into embedded, union, or list values, so a non-sensitive attribute or action argument that holds an embed with a sensitive? field (for example an accepted credentials embed carrying a token) is written to the version table in cleartext. This issue affects ash_paper_trail: from 0.3.0 before 0.7.0.	N/A	More Details
CVE-2026-77831	Inefficient Algorithmic Complexity vulnerability in ash-project ash_paper_trail allows a user who can submit a large array attribute to a paper-trailed create or update action to cause a denial of service through excessive CPU and memory use. With full-diff change tracking, AshPaperTrail.ChangeBuilders.FullDiff.ListChange pairs each prior array element against the new list by rebuilding the remaining-elements accumulator with acc ++ [tuple] on every step, copying the growing list each time, so the pairing scales cubically in the array length. Nothing bounds the length and the value comes straight from action input, so one request carrying a large accepted {:array, _} attribute forces tens of seconds of CPU and multi-gigabyte allocations. This issue affects ash_paper_trail: from 0.1.1 before 0.7.0.	N/A	More Details
CVE-2026-12717	An Improper Input Validation vulnerability in CData JDBC driver integration in Google Cloud BigQuery Data Transfer Service versions prior to 2026-05-01 on Google Cloud Platform allows an authenticated attacker to achieve remote code execution in the connector container and escalate privileges in the tenant project using crafted JDBC connection string parameters. This vulnerability was patched on 1 May 2026, and no customer action is needed.	N/A	More Details
CVE-2026-79619	On Linux, several OpenZFS ioctl authorization checks accept a capability held only within a user-created, unprivileged namespace as equivalent to real host privilege, allowing an unprivileged local user to perform operations that should require root. Affected operations include pool-administrative operations (eg create, import, destroy), pool event log access (zpool events) and fault injection (zinject). Exploiting the problem requires only that the local user is permitted to open /dev/zfs (governed by local device permissions) and that the kernel permits unprivileged user namespace creation. No prior access to the target pool or its underlying devices is needed.	N/A	More Details
CVE-2026-82724	Incorrect Authorization vulnerability in ash-project ash_phoenix invokes the SubdomainHook authorization callback with a nil tenant, so tenant-scoped access checks never see the tenant they are meant to enforce. AshPhoenix.LiveView.SubdomainHook.on_mount/4 attached a handle_params hook to assign the tenant and then immediately called handle_subdomain in the same on_mount. The tenant assign is only written when LiveView later runs handle_params, strictly after on_mount returns, so handle_subdomain read an unset assign and ran as apply(m, f, [socket, nil | a]). A consumer gate that halts when the user does not belong to the tenant instead evaluated nil, either crashing or taking a permissive branch, and it was never re-run once the real subdomain was assigned or on later navigations. The fix runs handle_subdomain inside the handle_params hook with the real tenant on every navigation. This issue affects ash_phoenix: from 2.1.26 before 2.3.25.	N/A	More Details
CVE-2026-82725	Authorization Bypass Through User-Controlled Key vulnerability in ash-project ash_phoenix lets an attacker who controls filter form parameters filter across relationships the resource author marked non-public, turning the returned rows into a boolean oracle over private related data. AshPhoenix.FilterForm resolved every relationship hop in the user-supplied path with Ash.Resource.Info.related/2, which traverses private relationships, and only checked the terminal field for publicity. parse_path_and_field/2 also rewrote a field naming a relationship into an extra path segment, so field=some_private_rel was accepted too. Both path and field come straight from form params, and the resulting ref went to Ash.Query.do_filter/2 without the public-only enforcement of Ash.Filter.parse_input/2. The fix resolves each hop with Ash.Resource.Info.public_relationship/2, rejecting the first non-public hop, and requires the terminal field to be public. This issue affects ash_phoenix: from 0.6.0-rc.1 before 2.3.25.	N/A	More Details
CVE-2026-	Cleartext Storage of Sensitive Information vulnerability in ash-project ash_paper_trail allows an attacker with read access to the generated version resource to recover the plaintext of sensitive? attributes. AshPaperTrail stores the values of tracked sensitive? attributes in the generated version resource's changes map, which is declared public? true and sensitive? false, so the values are returned by the version		More

75847	resource's default read action and printed in logs, inspect output, and error messages instead of being redacted. AshPaperTrail.Resource.Transformers.CreateVersionResource derives the changes map's sensitivity from the ignore_attributes list (the attributes excluded from changes) rather than from the tracked attributes actually stored in it, and ignore_attributes defaults to empty, so the flag is effectively always false. This issue affects ash_paper_trail: from 0.1.1 before 0.7.0.	N/A	Details
CVE-2026-82726	Permissive Regular Expression vulnerability in ash-project ash_phoenix lets a remote client select the tenant an Ash application uses, or degrade the request, by sending a crafted Host header. AshPhoenix.Helpers.get_subdomain/2 stripped the root domain with String.replace(host, ~r/.?#{root_host}/, ""). The root host was interpolated raw, so each . became a wildcard and any metacharacter a pattern, and the replace was global and unanchored, so a match was removed from anywhere in the string. With root_host example.com, Host: foo.exampleXcom.attacker.net returned the tenant foo.attacker.net. A metacharacter-bearing or nil root host degraded the pattern or raised on every request. The comparison was also case-sensitive, so TENANT.EXAMPLE.COM and EXAMPLE.COM slipped past the root-host allowlist. conn.host comes from the client Host header. The fix matches the root host case-insensitively and only as an exact trailing suffix. This issue affects ash_phoenix: from 2.1.26 before 2.3.25.	N/A	More Details
CVE-2026-82727	Generation of Error Message Containing Sensitive Information vulnerability in ash-project ash_phoenix writes the entire raw submitted param map into an exception message, so secrets submitted alongside a union form field leak into logs, crash reports and the dev error page. When AshPhoenix.Form.Auto builds a union sub-form and the submitted _union_type does not match a configured type, both raise sites built the message with inspect(params, pretty: true), embedding the full untrusted param map, and also inspected the internal union constraints[:types]. Because the message is constructed by the library rather than Phoenix's parameter logger, config :phoenix, :filter_parameters never redacts it. An attacker controls both the trigger and the contents: submitting %{"_union_type" => "nope", "password" => "..."} puts the password verbatim in the raised message. The fix reports only the offending _union_type and the valid type names, dropping the param and constraints dumps. This issue affects ash_phoenix: from 1.2.17 before 2.3.25.	N/A	More Details
CVE-2026-12587	The vulnerability allows the unauthorised generation of physical access QR codes due to the use of hard-coded credentials within the application. The generation mechanism uses the 'badge_number' parameter as the HMAC private key, the value of which remains static and is accessible via the API using the endpoint '/club/_id_club_/member/_id_member_/resamania_qr_info'. An attacker with access to this value and to the application’s cryptographic logic, which can be extracted by reverse engineering the APK as there is no code obfuscation, could generate valid QR codes indefinitely, even after the user has changed their password or logged out.	N/A	More Details
CVE-2026-53620	GROWI contains a vulnerability with an authorization bypass through user-controlled key in the bookmark folder APIs. If this vulnerability is exploited, an authenticated attacker could retrieve, tamper with, and/or delete the other user's bookmark data.	N/A	More Details
CVE-2026-68951	GROWI contains an incorrect authorization vulnerability. If this vulnerability is exploited, an unauthenticated attacker could retrieve the other user's bookmark data.	N/A	More Details
CVE-2026-64842	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-46684	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2026-80581	In the Linux kernel, the following vulnerability has been resolved: ASoC: SOF: ipc4-pcm: Continue the pipeline trigger in case of IPC timeout Ignore IPC errors for pipeline state change if the firmware state is crashed or the IPC has timed out. If the firmware has crashed the kernel still needs to go through the state changes to reset its internal to be able to correctly work the next time the DSP is booted up. The case with IPC timeout is a bit more problematic, but it has been rootcaused to be the result of system scheduling blockage and the firmware did actually received and handled the message, but the reply handling got blocked by issues outside of the SOF stack. So far the best way to handle this is to continue with setting the state.	N/A	More Details
CVE-2023-31249	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2026-6876	ServiceNow has remediated a sandbox escape security issue that was identified in the ServiceNow AI Platform. This security issue could allow an unauthenticated user to execute arbitrary code within the ServiceNow AI Platform, potentially leading to more access to the ServiceNow AI Platform than intended. ServiceNow deployed a security 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 Details
CVE-2026-	ServiceNow has remediated a SQL injection vulnerability that was identified in in the ServiceNow AI platform. This vulnerability could enable an unauthenticated user, in certain circumstances, to execute arbitrary SQL statements against the instance's underlying database and gain access to, or modify, instance data beyond what was intended. ServiceNow deployed a security update to hosted instances and	N/A	More

74820	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.		Details
CVE-2023-32648	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-32640	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-32631	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-32630	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-32287	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-32286	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-31270	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-31243	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2026-65931	LimeSurvey Community Edition 7.0.5 contains an authenticated improper authorization vulnerability in the survey menu entry creation endpoint. An authenticated user with only the global settings:read permission can directly invoke POST /index.php/admin/menuentries/sa/create and create new survey menu entries without the expected settings:update privilege. The endpoint also allows the attacker to submit menu IDs that the normal interface and intended update workflow restrict for non-superadministrators, enabling unauthorized changes to administrative navigation records. This issue affects LimeSurvey: 7.0.5.	N/A	More Details
CVE-2023-31202	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2026-81931	Unrestricted Upload of File with Dangerous Type in the product photo upload in Roskus Prospero Flow CRM before 5.16.0 allows an authenticated user holding the create product permission (routine Seller role) to execute arbitrary JavaScript in the application origin. The photo validation rule classifies the file only by its content (magic bytes) and rejects only a fixed list of PHP extensions, while ProductSaveController::save() names the stored file using the client-supplied extension and copies it into the public web root. A file that begins with an image header and carries an HTML extension passes validation, is stored under public/asset/upload/product/, and is served with a text/html content type, turning the upload into first-party stored script execution.	N/A	More Details
CVE-2023-31201	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-30761	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2026-17610	In SiSDK v2026.6.0 and earlier, high network traffic loads can cause a dropped ACK leading to a denial of service. This is only present for EFR32MG24 and EFR32MG26 devices running concurrent multiprotocol Zigbee and Thread.	N/A	More Details
CVE-2023-29496	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-28825	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-28822	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2026-38345	A Division-by-Zero vulnerability in the ff_sws_init_single_context function (/libswscale/utils.c) of FFmpeg N-122528-gdd2976b9e1 allows attackers to cause a Denial of Service (DoS) via a crafted input.	N/A	More Details
CVE-2026-66353	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in woylie doggo allows Reflected XSS. Doggo.normalize_value/2 in lib/doggo.ex returned date field values wrapped in {:safe, ...}, the Phoenix.HTML marker meaning "already escaped, emit verbatim", without escaping them, so the value reached the value attribute of the <input> rendered by the field component unchanged. Any application rendering <.field type="date"> over user-controlled params is affected through the ordinary Phoenix form round-trip, where a failed validation re-renders the submitted value. The pattern kept exactly the first ten bytes and discarded shorter values, capping a payload at ten bytes: enough to terminate the	N/A	More Details

	attribute and open an element or attach a short event handler, not enough to place attacker-chosen script inline. Only type="date" is affected. This issue affects doggo: from 0.1.0 before 0.14.8.		
CVE-2023-32733	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2026-78195	A Cross-Site Scripting (XSS) vulnerability in the WatchGuard Dimension Backup Historical Data feature allows an authenticated administrator user to execute arbitrary JavaScript in another user's browser.	N/A	More Details
CVE-2026-54687	n8n-nodes-sqlite3 is a node for operating a local SQLite database from n8n. Prior to 1.0.0, nodes/SqliteNode/v1/SqliteV1.node.ts exposes the db_path database file path as a node parameter that permits data expressions from upstream workflow input. A workflow author who maps untrusted input to db_path can allow a remote attacker to select which SQLite file the n8n process opens, enabling traversal outside the intended database location and potentially reading, creating, or overwriting files accessible to the process. This issue is fixed in version 1.0.0.	N/A	More Details
CVE-2026-37070	Incorrect access control in /vfm-admin/ajax/streamvid.php in Veno File Manager Project in 4.4.9 allows an authenticated attacker to read any uploaded files by other users as long as it knows the path and filename via a specially crafted GET request to the affected endpoint.	N/A	More Details
CVE-2026-37071	Arbitrary File Rename Leading to Privilege Escalation in Actions::renameFile() function in Veno File Manager Project 4.4.9 allows an authenticated attacker with 'reanme' permission to take over the super administrator account via a specially crafted POST request to the affected endpoint renaming the application configuration file and triggering a rebuild of configuration and resetting super administrator credentials to default values.	N/A	More Details
CVE-2026-37072	Veno File Manager Project Veno File Manager Project 4.4.9 is vulnerable to Incorrect Access Control in admin-head-updates.php.	N/A	More Details
CVE-2023-35135	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2026-47727	Trilium is an open-source hierarchical note-taking application. In versions prior to 0.104.0, the default-on "Safe import" filter fails to neutralize the shareTemplate relation because that relation is not marked as dangerous, allowing an attacker-supplied import archive to plant a server-side template that leads to remote code execution. The relation is omitted from the built-in list of dangerous attributes, so unlike other code-loading relations it is not disabled on import, and when the victim later publishes the imported note the public share renderer feeds the linked EJS code note's raw bytes into ejs.render, which compiles them in the server's Node process. An unauthenticated request to the shared note then executes the attacker's JavaScript with full access to require, process, the filesystem, and the network. This issue is fixed in version 0.104.0.	N/A	More Details
CVE-2026-48996	Trilium is an open-source hierarchical note-taking application. In versions up to and including 0.103.0, the default-on "Safe import" filter does not sanitize note titles, and the GeoMap note view interpolates a marker note's title into raw HTML that is rendered as innerHTML, allowing an attacker-supplied import archive to inject script that runs when the map is displayed. Because Safe import neutralizes scripts but never escapes titles, a note whose title contains an HTML event-handler payload survives the import and executes as soon as the victim opens the GeoMap that renders its marker. On the desktop client the Electron renderer runs with Node integration enabled, so the injected JavaScript escalates from cross-site scripting to full remote code execution on the victim's machine. This issue is fixed in version 0.104.0.	N/A	More Details
CVE-2026-53578	Trilium is an open-source hierarchical note-taking application. In versions up to and including 0.103.0, the default-on "Safe import" filter sanitizes HTML only for text notes and excludes the mindMap note type, whose JSON content is stored without sanitization, allowing an attacker-supplied import archive to embed a payload that renders as arbitrary HTML. A mind map node can carry a dangerouslySetInnerHTML property that the Mind Elixir library assigns directly to a node's innerHTML, so a malicious note survives Safe import and executes script as soon as the victim opens the imported mind map. On the desktop client the Electron renderer runs with Node integration enabled, so the injected JavaScript escalates from cross-site scripting to full remote code execution on the victim's machine. This issue is fixed in version 0.104.0.	N/A	More Details
CVE-2026-53579	Trilium is an open-source hierarchical note-taking application. In versions up to and including 0.103.0, the default-on "Safe import" filter sanitizes HTML only for text notes and excludes the book note type, whose content is stored without sanitization and later rendered as HTML, allowing an attacker-supplied import archive to embed a payload that executes as script. A book note's content is routed through the same rendering path as text notes and injected into the page with jQuery's html method when the note is shown as a grid-view preview card, so a malicious note survives Safe import and runs as soon as the victim opens the containing note. On the desktop client the Electron renderer runs with Node integration enabled, so the injected JavaScript escalates from cross-site scripting to full remote code execution on the victim's machine. This issue is fixed in version 0.104.0.	N/A	More Details
CVE-2023-35125	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-35122	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details

CVE-2023-34084	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-35063	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2026-55758	CC: Tweaked is a mod for Minecraft which adds programmable computers, turtles, and more to the game. Prior to 1.120.0, the SSRF protection in projects/core/src/main/java/dan200/computercraft/core/apis/http/options/AddressPredicate.java blocks the RFC 6052 64:ff9b::/96 NAT64 prefix but omits the RFC 8215 64:ff9b:1::/48 local-use prefix. On a dual-stack server using RFC 8215 NAT64, an unauthenticated user who can execute Lua code can use http.request or http.websocket with an address under 64:ff9b:1::/48 to reach loopback, RFC 1918, cloud metadata, or internal API endpoints because PrivatePattern.matches() does not classify the mapped IPv6 address as private. This issue is fixed in version 1.120.0.	N/A	More Details
CVE-2023-35059	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-35058	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-35000	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-34996	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-34428	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-34393	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-34313	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-28721	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-28719	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-28717	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2026-19317	An out-of-bounds read vulnerability in the WatchGuard Fireware OS iked process allows a remote unauthenticated attacker to create a Denial of Service (DoS) condition in VPN processing by sending specially crafted network traffic.	N/A	More Details
CVE-2023-24017	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2026-81851	A heap-based buffer overflow vulnerability in Fireware OS's iked process allows an authenticated administrator to crash the IKE daemon (iked), resulting in a denial of service, by saving a specially crafted configuration.	N/A	More Details
CVE-2023-24013	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2026-13086	A stack-based buffer overflow in the epm (Endpoint Protection Manager) service used by the deprecated Mobile Security feature in WatchGuard Fireware OS allows an unauthenticated remote attacker to execute arbitrary code.	N/A	More Details
CVE-2026-13108	WatchGuard Dimension is susceptible to a denial-of-service condition when an attacker sends a high volume of TCP SYN packets to the log listening service.	N/A	More Details
CVE-2026-19313	An heap overflow vulnerability in the WatchGuard Fireware OS iked process allows a remote unauthenticated attacker to execute arbitrary code by sending specially crafted network traffic.	N/A	More Details
CVE-2026-52776	Compliance-trestle (Trestle) is a tooling platform for managing compliance as code. In versions before 3.12.4 and versions 4.0.0 through 4.0.3, the URLSecurityValidator that guards trestle's remote-fetch paths against server-side request forgery can be bypassed to reach loopback, link-local, cloud-metadata, and internal network endpoints it was designed to block. The blocklist does not canonicalize IPv4-mapped IPv6 literals such as [::ffff:169.254.169.254], which resolve to IPv6Address objects that never match the blocked IPv4 ranges, and it does not block the unspecified address 0.0.0.0, which routes to local services on Linux and	N/A	More Details

	inside containers. An attacker who can supply or influence an OSCAL artifact that trestle fetches, such as a malicious profile whose imports reference one of these bypass URLs, can cause the HTTPSFetcher and SFTPFetcher paths to contact cloud instance-metadata services, loopback interfaces, or internal hosts. This issue is fixed in versions 3.12.4 and 4.1.0.		
CVE-2026-19315	A type confusion vulnerability in the iked process of WatchGuard Fireware OS allows a remote unauthenticated attacker to execute arbitrary code by sending specially crafted network traffic.	N/A	More Details
CVE-2026-19316	A double-free vulnerability in the WatchGuard Fireware OS iked process allows a remote unauthenticated attacker to create a Denial of Service (DoS) condition in VPN processing by sending specially crafted network traffic.	N/A	More Details
CVE-2026-19318	A stack-based buffer overflow vulnerability in the WatchGuard Fireware OS iked process allows a remote unauthenticated attacker to execute arbitrary code by sending specially crafted network traffic.	N/A	More Details
CVE-2023-28403	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-23905	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-22658	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-22431	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2026-78008	A buffer overflow vulnerability in the WatchGuard Fireware OS Management Web UI allows an authenticated administrator with network access to cause a denial of service (DoS) condition or potentially execute arbitrary code by sending specially crafted network traffic.	N/A	More Details
CVE-2026-78009	An out-of-bounds read vulnerability in the WatchGuard Fireware OS iked process allows a remote unauthenticated attacker to create a Denial of Service (DoS) condition in VPN processing by sending specially crafted network traffic.	N/A	More Details
CVE-2026-78010	A stack-based buffer overflow vulnerability in the WatchGuard Fireware OS iked process iallows a remote unauthenticated attacker to create a Denial of Service (DoS) condition in VPN processing by sending specially crafted network traffic.	N/A	More Details
CVE-2026-78011	An integer underflow vulnerability in the WatchGuard Fireware OS iked process allows a remote unauthenticated attacker to create a Denial of Service (DoS) condition in VPN processing by sending specially crafted network traffic.	N/A	More Details
CVE-2026-78047	A stored cross-site scripting (XSS) vulnerability in WatchGuard Dimension's task scheduling feature allows a low-privileged authenticated administrator to inject arbitrary HTML/JavaScript into these fields, which then executes in the browser session of any other user.	N/A	More Details
CVE-2026-78103	WatchGuard Dimension provides a client-side lock/unlock UI control for management changes. The server-side configuration endpoint does not enforce this lock/unlock workflow state, allowing an authenticated administrator to submit configuration changes directly to the endpoint without first completing the UI unlock step. This allows an authenticated read-write administrator session to bypass the intended editing workflow and overwrite configuration changes being made by another concurrent administrator session.	N/A	More Details
CVE-2023-24462	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2026-77358	cpp-httplib is a C++ header-only HTTP/HTTPS library. In versions 0.33.0 through 0.50.0, the TLS-enabled WebSocket client frees the TLS session before closing the WebSocket that still uses it, producing a use-after-free. In WebSocketClient::shutdown_and_close the SSL object is freed and the pointer cleared, but the subsequent WebSocket close still sends a close frame through the SSL socket stream, which holds a raw copy of the now-dangling session pointer and reads from and writes to the freed memory. The same freed-then-used ordering is reachable through the client's destructor and its connect path, so ordinary teardown of a secure WebSocket connection triggers the defect. This issue is fixed in version 0.50.1.	N/A	More Details
CVE-2026-77341	cpp-httplib is a C++ header-only HTTP/HTTPS library. In version 0.49.0, the chunked-response trailer output path writes trailer header names and values directly to the socket without validating them, allowing CRLF sequences in a trailer field to inject additional headers or split the HTTP response. Unlike every other header-writing path in the library, the trailer-writing code applies none of the field-name and field-value checks that reject carriage return and line feed, so an application that places attacker-influenced data into a chunked response trailer emits attacker-controlled CRLF onto the wire. This enables HTTP response splitting, letting an attacker forge response headers or inject a second response. This issue is fixed in version 0.50.0.	N/A	More Details
CVE-2023-24541	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details

CVE-2023-27924	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-27885	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-27884	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-27883	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-27880	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-27528	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2026-5706	In Bluetooth Mesh SDK 6.1.4 and earlier, malformed extended advertisements can trigger out-of-bounds writes leading to stack corruption and remote code execution. These messages must come from a device that has already joined the network. Only provisioners supporting extended advertisements may be impacted.	N/A	More Details
CVE-2026-61783	Wazuh is an open-source security platform providing unified XDR and SIEM protection for endpoints and cloud workloads. In versions 4.14.0 through 4.14.6, an authenticated low-privilege user can read the cluster secret from the manager configuration because the logic that masks sensitive values is disabled by any update-config RBAC rule, including an explicit deny. The mask_sensitive_config() decorator applies masking only when _has_update_permissions() returns false, but that gate treats a user as able to update the config whenever a manager:update_config or cluster:update_config rule exists, without ever checking whether the rule's effect is allow or deny. Because a deny rule is stored as a real entry, a read-only account that is hardened by explicitly denying config edits is counted as having update permission, which turns masking off. A single authenticated GET request to the configuration endpoint with raw=true then returns the verbatim ossec.conf XML with cluster.key in clear, whereas an otherwise identical account without the deny rule sees the value masked. This issue is fixed in version 4.14.7.	N/A	More Details
CVE-2023-27511	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2026-68929	FastGPT is an open-source LLM platform for building AI applications on a knowledge base. In versions prior to 4.15.2, the WeChat (iLink) share-channel endpoints authorize requests using only the public shareId, with no authenticated identity or team-ownership check. As a result, an unauthenticated attacker who knows a victim team's shareId can take that team's WeChat bot offline or hijack the channel to their own bot: the logout endpoint is gated only by an existence check yet wipes the outLink's stored WeChat token, and the QR-code status endpoint performs no authorization at all and writes attacker-supplied bot credentials into the outLink identified by shareId. By generating a QR for a victim shareId, scanning it with their own WeChat, and calling the status endpoint, an attacker binds the victim team's app to the attacker's bot, exposing the app's private responses, displacing the legitimate binding, and consuming the victim's resources. The shareId is exposed in every shared chat URL, iframe, and embed, so it is not a secret. This issue is fixed in version 4.15.2.	N/A	More Details
CVE-2023-27393	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-27381	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-27302	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-27299	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-26594	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-25778	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-25079	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-24596	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-24543	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details

CVE-2026-37069	Absolute Path Disclosure in /vfm-admin/assets/zipstream/grandt/relativepath/RelativePath.Example1.php in Veno File Manager Project 4.4.9 allows an unauthenticated attacker to know in which system directory the application code is running by sending a GET request to the endpoint.	N/A	More Details
CVE-2026-37068	Arbitrary file write in /vfm-admin/index.php?section=translations&action=update in Veno File Manager Project 4.4.9 allows an authenticated user with the role of super administrator to overwrite any php file in the application via a specially crafted POST request to the affected endpoint.	N/A	More Details
CVE-2026-37066	Path traversal leading to Arbitrary File Read in /vfm-admin/index.php and /vfm-admin/ajax/streamvid.php in Veno File Manager Project 4.4.9 allows and authenticated attacker with super administrator role to disclose sensitive information via two specially crafted http requests (POST and GET) to the affected endpoints.	N/A	More Details
CVE-2023-42432	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-43613	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-43607	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-43486	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-43483	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-42779	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-42778	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-42777	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-42767	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-42434	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-42430	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2026-56652	Dool in versions up to 1.3.8 is vulnerable to a CSV injection vulnerability when exporting data to a CSV file, as it fails to sanitize cell content beginning with special formula characters like =, +, -, or @. A local attacker can exploit this by running a process with a crafted name starting with =, which injects malicious formulas into the CSV output that execute when a victim opens the file in a spreadsheet application. The issue was addressed by pull request #117	N/A	More Details
CVE-2023-41959	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-41371	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-41370	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-41087	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-41083	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-40746	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-40538	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-40157	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is		More

40149	Unused	N/A	Details
CVE-2023-43759	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-45211	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-45214	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-45216	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-46703	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-46709	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-46710	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-47176	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-47205	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-47206	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-47208	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-47214	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-48337	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-48370	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-49116	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-49592	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-49601	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-49605	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-49720	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-46101	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-45848	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-45739	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-45313	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2026-56651	Dool in versions up to 1.3.8 is vulnerable to symlink following when the "--devel" flag is used, as the application opens a log file without the "O_NOFOLLOW" flag. A local attacker can exploit this by creating a symlink at the expected log file path pointing to a sensitive file, causing dool to truncate and overwrite the target file with log data, which is especially impactful if dool is run with elevated privileges. The issue was addressed by pull request #116	N/A	More Details

CVE-2023-40147	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2026-37065	Veno File Manager Project 4.4.9 is vulnerable to Arbitrary File Deletion in /vfm-admin/index.php?section=translations&action=update&remove=.	N/A	More Details
CVE-2026-81817	Affected versions of Flowintel contain an insecure direct object reference / broken object-level authorization issue across numerous task endpoints. The routes generally received both a case identifier and a task identifier, but previously they did not enforce that the task actually belonged to the supplied case. As a result, an authenticated user with editor-level access to one case could potentially substitute the ID of a task from another case and invoke operations against that foreign task. The patch introduces task_case_bound_required, which loads both objects and returns 404 unless the task belongs to the requested case. This protection is applied to edit, delete, note, assignment, status, file, export, MISP-linking, subtask, external-reference, and other task-related endpoints. The fix also adds explicit checks that a requested note_id belongs to the current task before returning or exporting it, closing related cross-object access paths. Version impacted =>3.3.0	N/A	More Details
CVE-2023-36863	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-36856	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-36855	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-36852	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-36491	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-35988	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-35771	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-35770	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-35768	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2026-81818	Affected versions of Flowintel contain an authorization flaw in the administrative user-edit API. The existing authorization check correctly prevented an organization administrator from editing users in another organization, but it did not prevent them from editing a full administrator within their own organization. As a result, an org admin could modify that full administrator account, including changing its password. The upstream commit explicitly describes the issue as: “Org admin can change the password of a full admin in the same organization.” The fix adds a higher-privilege boundary check: if user_to_edit.is_admin(): return ... 403 so organization administrators can no longer modify full administrator accounts. Version impacted >=3.3.0	N/A	More Details
CVE-2026-64896	Debug and Test Interface With Improper Access Control vulnerability in Johnson Controls T2000 allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects T2000: before 31.6.	N/A	More Details
CVE-2026-81819	Affected versions of Flowintel expose the /my_assignment/user API endpoint to any authenticated API user. The endpoint accepts a user_id parameter identifying the user whose assignments should be returned, but previously had no role restriction beyond general API authentication. As a result, a lower-privileged authenticated user could potentially query another user’s assignment information by supplying that user’s identifier. The fix changes: method_decorators = [api_required] to: method_decorators = [admin_or_org_admin_required, api_required] so only administrators or organization administrators can perform cross-user assignment queries. Version impacted =>3.3.0	N/A	More Details
CVE-2026-81820	Affected versions of Flowintel construct timeline HTML using attacker-controllable MISP object fields such as: * object UUID; * object name; * attribute value; * attribute type; * comment; * first/last seen values; * IDS flag. Those values were concatenated directly into HTML strings before rendering. The upstream commit explicitly states that DOMPurify removed XSS vectors but still allowed other HTML elements, such as forms, through. The fix replaces direct string interpolation with DOM construction via document.createElement() and assigns all attacker-controlled values using textContent. The headline is similarly converted to escaped HTML through a temporary element. Version impacted =>3.3.0	N/A	More Details
CVE-2026-	Affected versions of Flowintel do not revoke existing authenticated sessions when a user’s password is changed. This means that if an attacker already possesses a valid session—for example, from prior access or a stolen session token—the victim changing their password does not terminate that attacker’s access.		More

81826	The session remains usable until it expires naturally. The upstream commit describes this directly as: “session keeps working until it expires.” The fix detects password changes and explicitly invokes _invalidate_user_sessions(user.id) after the database update. This is applied in both edit_user_core() and admin_edit_user_core(). Version impacted >=3.3.0	N/A	Details
CVE-2026-81827	Affected versions of Flowintel incorrectly attempted to validate login email addresses by calling Email(email). That does not perform WTForms field validation; it merely constructs a validator object. Consequently, malformed attacker-controlled email input could continue through the login process and be written to security-relevant logs. The vulnerable code inserted the supplied email into both a warning log and the custom audit logger. Since CR/LF characters were not escaped, an unauthenticated attacker could potentially inject additional physical log lines or forge misleading log entries. The patch corrects the validation call to Email()(form, form.email), changes the standard logging call to parameterized logging, and introduces _sanitize_log_fragment() so carriage returns and line feeds are encoded instead of creating new records. Version impacted >=3.3.0	N/A	More Details
CVE-2023-35766	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2026-18885	ServiceNow has remediated a code injection vulnerability that was identified in the ServiceNow AI platform. This vulnerability could enable an unauthenticated user, in certain circumstances, to execute arbitrary code in the ServiceNow platform and gain access to, or modify, instance data beyond what was intended. ServiceNow deployed a security 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 Details
CVE-2026-18886	ServiceNow has remediated an improper access control vulnerability that was identified in the ServiceNow AI platform. This vulnerability could enable an unauthenticated user, in certain circumstances, to create or modify instance data beyond what was intended, resulting in privilege escalation. ServiceNow deployed a security update to hosted instances and ServiceNow provided the update to our partners and self-hosted customers. We are not currently aware of 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 Details
CVE-2023-35761	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-35190	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-38134	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-38260	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-38539	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-38540	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2026-71401	An integer underflow was found in the DHCPv4 packet capture code of wicked. ni_capture_inspect_udp_header() in src/capture.c does not verify that the IP total length field (ip_len) is at least as large as the IP header length (ihl) before subtracting the header length. An unauthenticated attacker on the same network can thereby trigger an out-of-bounds read past the receive buffer in the wicked DHCPv4 client (wickedd-dhcp4), which can crash the daemon depending on the process memory layout. No information disclosure has been demonstrated. This issue affects wicked up to and including version 0.6.80.	N/A	More Details
CVE-2023-39942	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-39940	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2026-78251	DJI drones contain an FTP service that uses hardcoded credentials shared across affected models and permits authenticated users to upload files without limits on file size, file count, or total storage consumed in **/blackbox/upgrade/**, as well as overwrite existing files in that directory. An attacker with access to the drone's internal network or USB RNDIS interface can exhaust the available storage, preventing the aircraft from writing flight records, logs, and telemetry and potentially preventing subsequent firmware updates. Uploaded files persist across reboot and factory reset. Affected models are DJI Neo until 01.00.0400, DJI Neo 2 until 01.00.0500, DJI Flip until 01.00.1200, DJI Air 3 until 01.00.1600, DJI Air 3S until 01.00.1400, DJI Avata 2 until 01.00.0400, DJI Avata 360 until 01.00.0300, DJI Mavic 3 until 01.00.1400, DJI Mavic 3 Classic until	N/A	More Details

	01.00.0800, DJI Mavic 3 Pro until 01.01.0700, DJI Mavic 4 Pro until 01.00.0500, DJI Mini 2 until 01.07.0200, DJI Mini 3 until 01.00.0500, DJI Mini 3 Pro until 01.00.0900, DJI Mini 4 Pro until 01.00.1100, and DJI Mini 5 Pro until 01.00.0600. Remediation requires a firmware update from the vendor.		
CVE-2026-79653	In Eclipse SW360 versions 19.0.0, 19.1.0, 19.2.0, 20.0.0, 20.1.0, if the system is configured to use file system storage with config key enable.attachment.store.to.file.system, the attacker can manipulate the filename upon upload and can essentially cause arbitrary file path traversal. The immediate workaround is to disable enable.attachment.store.to.file.system or update to fixed versions.	N/A	More Details
CVE-2026-79718	Reflected XSS in Netron versions <=9.1.2 on desktop application through unsanitized node names allows an attacker to hide certain nodes, perform port scanning or abuse a Chrome n-day to achieve Remote Code Execution.	N/A	More Details
CVE-2026-79719	Reflected XSS in Netron versions <=9.1.2 on desktop application through unsanitized node names allows an attacker to hide certain nodes, perform port scanning or abuse a Chrome n-day to achieve Remote Code Execution.	N/A	More Details
CVE-2026-79988	The Twig sandbox mechanism in Craft CMS is configured to allow dangerous functionality from the Yii framework, leading to authenticated RCE similar to previously disclosed vulnerabilities.	N/A	More Details
CVE-2023-39931	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-39449	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-39430	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-39426	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-39232	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-39229	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-39225	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-38656	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-38578	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-38577	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-38567	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2026-78174	WatchGuard Dimension records unredacted session identifiers for logged-in users in its web UI diagnostic log. A low-privileged Dimension Administrator can retrieve this log and extract a Super Administrator's session token while that administrator is logged in, enabling account takeover.	N/A	More Details
CVE-2026-78495	A server-side request forgery (SSRF) vulnerability WatchGuard Dimension Remote Backup Connection Test configuration allows an authenticated privileged attacker to enumerate exposed network services on adjacent network systems.	N/A	More Details
CVE-2026-54606	SunEditor is a lightweight and powerful WYSIWYG editor in vanilla JavaScript with no dependencies. Prior to 3.1.4, the SunEditor Embed plugin in src/plugins/modal/embed.js parses attacker-controlled raw embed HTML with DOMParser and processes the resulting DOM nodes. When an external script element follows a valid iframe, the plugin recreates a script element from the attacker-controlled src attribute and appends it to the live DOM, causing JavaScript execution in the editor page. If an application stores or reflects SunEditor content without additional backend sanitization, an attacker who can submit embed HTML can trigger stored or reflected cross-site scripting when another user opens, previews, renders, or edits the content, enabling access to page data and account actions as the victim. This issue is fixed in version 3.1.4.	N/A	More Details
CVE-2023-22364	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-22446	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details

CVE-2023-22445	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-22437	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-22434	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-22433	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-22430	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-22426	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-22423	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-22420	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-22352	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-27503	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-22343	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2023-22328	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2026-13761	Pega Platform versions 7.1.0 through 25.1.2 are affected by an improper validation of inputs that are used for loop conditions, potentially leading to a denial of service or other consequences because of excessive looping.	N/A	More Details
CVE-2026-14942	Rejected reason: This CVE ID was assigned to a reported vulnerability in the Customer Reviews for WooCommerce WordPress plugin and was never published. The report was withdrawn: the precondition it depends on, an attacker obtaining a review form identifier belonging to a customer they do not already have access to, could not be demonstrated. No advisory was issued for this ID.	N/A	More Details
CVE-2026-19412	This vulnerability exists in the CP Plus CP-XR-DE21-S Router due to the presence of hardcoded HTTP Digest authentication credentials in the firmware that are identical across all devices running the affected firmware. An attacker with access to the local network could exploit this vulnerability by obtaining the hardcoded authentication information from the firmware. Successful exploitation of this vulnerability could allow the attacker to gain unauthorized administrative access and perform privileged operations on the targeted device.	N/A	More Details
CVE-2026-37236	grpc-gateway v2.28.0 is vulnerable to Incorrect Access Control. The application processes the X-HTTP-Method-Override header in ServeMux.ServeHTTP without restricting allowed methods. When a POST request with Content-Type application/x-www-form-urlencoded includes this header, the request method is rewritten to an arbitrary attacker-supplied value before routing. This allows bypassing method-based access controls enforced by upstream proxies or WAFs.	N/A	More Details
CVE-2023-22289	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2026-16895	A logic vulnerability (fail-open condition) has been identified within the Metasploit Framework's JSON-RPC web service interface. When an exception occurs during the database health check (db.check) and the environment variable MSF_WS_JSON_RPC_API_TOKEN is not explicitly set, the application resets the internal state flag msf.auth_initialized to false. The ApiToken Warden authentication strategy misinterprets this false value as an indicator that authentication is not initialized or required, thereby granting unauthenticated local access to the JSON-RPC request dispatcher.	N/A	More Details
CVE-2026-19398	“unsupported-when-assigned.” An out-of-bounds write in the SmiFlash SMM module of ASUS FA507NU and FA507NV BIOS allows a local administrator to cause a system crash (BSOD) or BIOS corruption via a crafted software SMI (SW SMI) request with an oversized length value.Refer to the ' Security Update for ASUS FA507NV / FA507NU BIOS ' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2023-23544	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details

CVE-2023-27508	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2026-78498	A server-side request forgery (SSRF) vulnerability WatchGuard Dimension Email Server Test configuration allows an authenticated privileged attacker to enumerate exposed network services on adjacent network systems.	N/A	More Details
CVE-2026-80705	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: check if dml21_add_phantom_plane() is successful Verify that the phantom plane was allocated to avoid a later segfault. (cherry picked from commit 5adb54abe5a8e82cbff7f8806db30a5f4924329f)	N/A	More Details
CVE-2026-77035	Joomla Extension - joomlaeventmanager.net - Cross-user event and venue takeover through forged form fields in Joomla Event Manager < 5.0.1 - A registered user with edit-own rights (the eventowner=1 setting or core.edit.own) can POST another user's record id together with their own id as created_by and take over that record.	N/A	More Details
CVE-2026-80695	In the Linux kernel, the following vulnerability has been resolved: hwmon: (sht3x) Fix unaligned accesses Sashiko reports: In sht3x_update_client(), the 16-bit temperature and humidity values are extracted from a stack-allocated byte array using be16_to_cpup(). The pointers passed to this function are calculated as buf and buf + 3. Since the difference between the two pointers is an odd number of bytes, at least one of them is guaranteed to be at an unaligned offset. This will trigger an alignment fault on strict-alignment architectures such as ARMv5 or SPARC, resulting in a kernel panic. Fix the problem by using get_unaligned_be16() instead of be16_to_cpup(), and put_unaligned_be16() instead of cpu_to_be16().	N/A	More Details
CVE-2026-77034	Joomla Extension - joomlaeventmanager.net - Unauthenticated article overwrite and force-publish in Joomla Event Manager < 5.0.1 - Any visitor holding their own session token can republish and overwrite an article associated with an event.	N/A	More Details
CVE-2026-80697	In the Linux kernel, the following vulnerability has been resolved: erofs: ensure valid f_path for page cache sharing Previously, backing files for page cache sharing were set up with f_path left as NULL (only f_inode was valid). It worked, but a recent mincore fix relies on f_path.mnt and crashes (found by "erofs/028" on 7.2-rc4): BUG: kernel NULL pointer dereference, address: 0000000000000018 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: Oops: 0000 [#1] SMP PTI CPU: 3 UID: 0 PID: 675528 Comm: fincore Not tainted 7.2.0-rc4-00002-g[]-dirty #1 PREEMPT(lazy) Hardware name: Red Hat KVM, BIOS 1.16.0-4.al8 04/01/2014 RIP: 0010:__do_sys_mincore+0xc0/0x2c0 ... Specify valid paths using valid disconnected dentries together with erofs_ishare_mnt instead of leaving f_path empty, so they are more like real backing files in a pseudo filesystem and standard backing_file_open() can be used directly.	N/A	More Details
CVE-2026-80698	In the Linux kernel, the following vulnerability has been resolved: dmaengine: idxd: fix double free of wq, engine, and group structs The release callbacks for wq, engine, and group devices (idxd_conf_wq_release, idxd_conf_engine_release, idxd_conf_group_release) each call kfree() on the enclosing struct. The setup error paths and cleanup functions also call kfree() explicitly after put_device(), producing a double free whenever put_device() drops the reference count to zero and fires the release. In the setup functions, device_initialize() is called before device_add(), so the reference count is exactly 1 at the error sites. put_device() unconditionally fires the release, which frees the struct; the subsequent explicit kfree() then operates on freed memory. For idxd_setup_wqs(), the wq release callback also owns opcap_bmap and wqcfg. The error unwind additionally freed those fields explicitly before calling put_device(), causing further double frees on both. Remove the redundant explicit kfree() calls from all setup error paths and cleanup functions for wq, engine, and group structs, delegating sole ownership of those allocations to the release callbacks.	N/A	More Details
CVE-2026-80699	In the Linux kernel, the following vulnerability has been resolved: KVM: arm64: vgic: Avoid double-deactivate of IRQs in the nested context In the nested state, the physical interrupt has already been deactivated through the HW bit in the LR. The extra deactivation would be harmless but can hit an errata case on AmpereOne, so avoid it here. On AmpereOne, deactivating a physical interrupt through ICC_DIR_EL1 or ICC_EOIR1_EL1 (depending on EOImode) which is not active, but is the highest priority pending interrupt causes the cpu to lose the interrupt pending state and also prevents the delivery of future interrupts.	N/A	More Details
CVE-2026-80701	In the Linux kernel, the following vulnerability has been resolved: drm/vmwgfx: enforce cursor size limits for MOB cursors vmw_cursor_plane_atomic_check() bounds cursor width and height only on the legacy update path; the SVGA_CAP2_CURSOR_MOB path -- the default on modern hosts -- accepts any size. When the requested size exceeds SVGA_REG_CURSOR_MAX_DIMENSION or SVGA_REG_MOB_MAX_SIZE, vmw_cursor_mob_get() returns -EINVAL and leaves vps->cursor.mob NULL. Its return value is then discarded in vmw_cursor_plane_prepare_fb(), so the subsequent vmw_cursor_update_mob() calls vmw_bo_map_and_cache(NULL) and oopses inside vmw_bo_map_and_cache_size() on the tbo.base.size load. Reachable from any DRM master via DRM_IOCTL_MODE_CURSOR2 with a sufficiently large width or height (e.g. cursor_max_dim + 1). Reject oversized cursors in atomic_check for both MOB-backed cursor update types. The MOB byte-size limit only applies to the SVGA_CAP2_CURSOR_MOB path (vmw_cursor_mob_size() returns 0 for GB_ONLY); compute the required MOB size in 64-bit to avoid overflow when very large dimensions are requested. In prepare_fb only call vmw_cursor_mob_get()/_map() for VMW_CURSOR_UPDATE_MOB -- the GB_ONLY path uses bo->map.virtual directly and would otherwise be silently downgraded to NONE on hosts without SVGA_CAP2_CURSOR_MOB (where vmw_cursor_mob_get() always returns -EINVAL). Degrade the update to NONE if vmw_cursor_mob_get() or vmw_cursor_mob_map()	N/A	More Details

	fails so the update path does not run with a NULL backing MOB.		
CVE-2026-80703	In the Linux kernel, the following vulnerability has been resolved: drm/amdkfd: Fix missing authorization check in KFD_IOC_DBG_TRAP_DISABLE Prevent unauthorized termination of active GPU debug sessions. Previously, users with /dev/kfd access could terminate another process's debug session without proper ownership or ptrace authorization. (cherry picked from commit 4db4c5ffd5585b72622ecf6ffedf2da258ee23f5)	N/A	More Details
CVE-2026-80704	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: use proper context for logging The same as the rest of the code, get_ss_info_from_atombios() uses calc_pll_cs->ctx->logger for logging. But calc_pll_cs->ctx is initialized only later in calc_pll_max_vco_construct(). Therefore, any output using DC_LOG_SYNC() leads to a NULL pointer deference in get_ss_info_from_atombios(). According to Sashiko, the very same problem exists in dce112_get_pix_clk_dividers() and dcn3_get_pix_clk_dividers() too. To avoid accessing the NULL context, use clk_src->base.ctx->logger everywhere. That context in base is initialized earlier in dce110_clk_src_construct() and dce112_clk_src_construct(). Before get_ss_info_from_atombios() or Sashiko's get_pix_clk_dividers functions above are actually called. This is done by redefining DC_LOGGER to CTX->logger. Before: dce110_clk_src_construct() did: -> sets clk_src->base.ctx = ctx; -> ss_info_from_atombios_create() -> get_ss_info_from_atombios() <- uses calc_pll_cs->ctx # BOOM -> calc_pll_max_vco_construct() <- sets calc_pll_cs->ctx After: dce110_clk_src_construct() does: -> sets clk_src->base.ctx = ctx; -> ss_info_from_atombios_create() -> get_ss_info_from_atombios() <- uses clk_src->base.ctx (cherry picked from commit 6f16fcbb0c46a87e3d9685407e906573d60104b0)	N/A	More Details
CVE-2026-80708	In the Linux kernel, the following vulnerability has been resolved: s390/zcrypt: Fix missing mem scrub at clear key import in cca_clr2cipherkey() The helper function _ip_cprb_helper() uses internal buffer memory for building and processing CPRBs. After use this buffer was never scrubbed which could lead to leaving for example clear key material in memory which could be exposed via tricky reuse of this same memory. Extend the _ip_cprb_helper() function with another parameter 'scrub' used to steer scrubbing of this buffer. So now the caller has the opportunity to decide if scrubbing is needed or not. Extend the clear key to secure key token import process in function cca_clr2cipherkey() to tell the helper function from above to scrub the cprb buffer when the clear key value is part of the request data. Add explicit scrubbing on return from function cca_clr2cipherkey() for the random EXOR buffer and the cprb buffer. Overall this cleans the internal used buffer in case of clear key import to prevent sensitive data to get exposed.	N/A	More Details
CVE-2026-81733	WWBN AVideo through 30.0 (and master up to commit 4cb576e) contains a cross-site request forgery vulnerability in plugin/Live/myLiveControls.save.json.php. The endpoint only checks that a user is logged in and processes customUrl, customMessage, and autoRedirect parameters from $_REQUEST via a GET request without enforcing a CSRF token or origin check. An attacker who lures a logged-in streamer to a malicious page can silently change the live-channel viewer-redirect settings (persisted in users.externalOptions), causing viewers to be redirected to a phishing site or shown a spoofed message.	N/A	More Details
CVE-2026-80711	In the Linux kernel, the following vulnerability has been resolved: power: supply: max17040: handle missing status supplier MAX17040 does not report charger state itself, so the driver forwards POWER_SUPPLY_PROP_STATUS to a supplier power supply. If no supplier is registered, power_supply_get_property_from_supplier() returns -ENODEV and leaves the output value untouched. max17040_get_property() currently ignores that error and returns success, so userspace can read an uninitialized status value from the battery power supply. This happens on systems that use the fuel gauge without a charger supplier relationship in firmware. Return POWER_SUPPLY_STATUS_UNKNOWN when no supplier provides STATUS, and propagate other supplier lookup errors.	N/A	More Details
CVE-2026-80715	In the Linux kernel, the following vulnerability has been resolved: igc: remove napi_synchronize() in igc_down() When an AF_XDP zero-copy application is killed abruptly, the XSK pool is torn down but NAPI keeps polling. igc_clean_rx_irq_zc() then returns the full budget on every poll, so napi_complete_done() never clears NAPI_STATE_SCHED. igc_down() calls napi_synchronize() before napi_disable(), so it spins forever waiting for that bit and the interface never goes down. Drop the napi_synchronize() and let napi_disable() do the job -- it sets NAPI_STATE_DISABLE, which forces the stuck poll to complete. Reorder it ahead of igc_set_queue_napi() so the NAPI mapping is cleared only after polling has stopped, matching the recent igb fix b1e067240379.	N/A	More Details
CVE-2026-80719	In the Linux kernel, the following vulnerability has been resolved: mm: mglru: fix stale batch updates after memcg reparenting The mglru page table walker batches per-generation size deltas in walk->nr_pages while walking page tables without holding the lruvec lock. The reset_batch_size() later folds those deltas into walk->lruvec under the lruvec lock. The page table walker can run concurrently with the memcg reparenting path as follows: CPU0 CPU1 ==== ==== walk_mm --> walk_page_range --> update_batch_size --> walk->nr_pages += delta mem_cgroup_css_offline --> memcg_reparent_objcgs --> lock lruvec lru_gen_reparent_memcg --> reparent child folios to parent unlock lruvec lock lruvec reset_batch_size --> child lrugen->nr_pages += delta This will trigger the following warning in lru_gen_exit_memcg(): VM_WARN_ON_ONCE(memchr_inv(lruvec->lrugen.nr_pages, 0, sizeof(lruvec->lrugen.nr_pages))); And the user-visible impact of underestimated nr_pages in MGLRU was premature OOMs because MGLRU does not try to reclaim memory when nr_pages reaches zero, but there are still more pages. To fix it, make reset_batch_size() check CSS_DYING under RCU before flushing the pending batch. A non-dying memcg keeps the original lruvec stable against RCU-delayed offlining; a dying memcg redirects the deltas to the first non-dying ancestor.	N/A	More Details

CVE-2026-18918	In Eclipse Lyo versions 2.0.0 to 7.0.0, OAuth server authorization checks can be bypassed when the 2-legged auth is supported by the server. In those cases, application that based their authz filters upon Lyo-provided `AbstractAdapterCredentialsFilter`, are vulnerable. An attacked can create a provisional trusted client (valid use-case) but then it can be used as a trusted client immediately without requiring the administrator approval to clear the provisional status. The 3-legged path requiring user interaction is not vulnerable and rejects provisional clients.	N/A	More Details
CVE-2026-78070	Joomla Extension - digital-peak.com - Authenticated, privileged blind SQL injection in DP Calendar 5.5.0 - 10.11.2 - Saving an article can trigger a blind SQL injection with content plugin, needs update permission for articles.	N/A	More Details
CVE-2026-78071	Joomla Extension - digital-peak.com - Authenticated, privileged stored XSS in DP Calendar 7.0.0 - 10.11.2 - Location title is rendered in data attribute without escaping leads to XSS, needs create permission in DPCalendar.	N/A	More Details
CVE-2026-78072	Joomla Extension - Jefferson49 - Unauthenticated blind SQLi in Sexy Polling Reloaded < 5.6.1	N/A	More Details
CVE-2026-78073	Joomla Extension - mrvinoth.com - Reflected XSS in All Video Share 1.0.0-4.5.0 - Various user supplied inputs lacked escaping, leading to reflected XSS vectors	N/A	More Details
CVE-2026-81732	WWBN AVideo through version 30.0 fails to enforce authentication on the report4.json.php and report4.1.json.php endpoints, allowing unauthenticated access to user registration statistics. Attackers can send GET requests to these endpoints to retrieve daily and cumulative user-registration counts without any session or authorization.	N/A	More Details
CVE-2026-80183	In OpenStack Keystone before 29.0.3, any authenticated user holding role:reader on any project can list every project-scoped role assignment under any domain by passing a domain ID as scope.project.id with include_subtree to the GET /v3/role_assignments endpoint. The domain's project record has domain_id=null, causing the policy domain_id check to pass for any caller. With include_names, the response discloses the names and home-domain IDs of every user, group, project, and role involved. The literal "default" domain ID works against any deployment created with keystone-manage bootstrap. An attacker can harvest domain IDs from the response and repeat the query to map role assignments across the entire cloud. This is caused by misuse of "None" in list_role_assignments_for_tree.	N/A	More Details
CVE-2026-58106	CVE-2025-40843 https://github.com/advisories/GHSA-5xf2-f6ch-6p8r was fixed by replacing unchecked strcpy() with a bounded safe_strcpy() helper. At ldlogger-tool-gcc.c:129 the destination passed to that helper is fullPath + 2, but the size passed down is the full PATH_MAX. safe_strcpy() is strncpy(), which NUL-pads the destination out to the whole n, so this site writes 4096 bytes into the 4094 that remain — a 2-byte stack overflow on every invocation, independent of the input path's length. This issue affects CodeChecker: through 6.28.2.	N/A	More Details
CVE-2026-58107	CodeChecker's massStoreRun processing path performs one-shot decompression of attacker-controlled, Base64-encoded zlib data without enforcing a maximum decompressed size. An authenticated user with permission to store analysis runs can submit a highly compressed payload that expands to a significantly larger byte sequence. Because the entire decompressed output is materialized in memory before being written to a temporary file, a sufficiently large payload may exhaust process or host memory and consume substantial disk space, resulting in denial of service.	N/A	More Details
CVE-2026-75118	A pre-authentication stack-based buffer overflow vulnerability exists in the http_gdpr_decrypt function of TL-MR100 V3.20 due to insufficient bounds checking of encrypted requests to the /cgi/login endpoint. An adjacent unauthenticated attacker with access to the router's web management interface can trigger memory corruption and potentially achieve arbitrary code execution. Successful exploitation can overwrite saved control-flow data on the httpd process stack prior to authentication, resulting in a service crash or potential arbitrary code execution in the context of the affected process.	N/A	More Details
CVE-2026-55520	Protego is a pure-Python robots.txt parser with support for modern conventions. Prior to 0.6.2, protego._urlpattern._URLPattern._prepare_pattern_for_regex translates every asterisk in an Allow or Disallow directive into a lazy regular-expression wildcard, so a directive containing many asterisks creates exponential backtracking. After protego.Protego.parse processes a crafted robots.txt file, protego.Protego.can_fetch can spend an attacker-controlled period matching a near-miss URL and deny service to the crawler. The vulnerable path is src/protego/_urlpattern.py in the _URLPattern match logic. This issue is fixed in version 0.6.2.	N/A	More Details
CVE-2026-55673	PowSyBl (Power System Blocks) is a framework to build power system oriented software. Prior to 7.2.2, UnixLocalCommandExecutor and WindowsLocalCommandExecutor concatenate command arguments and environment variables into strings interpreted through bash -c or cmd /c without sufficient escaping. Attacker-controlled values reaching UnixLocalCommandExecutor.execute, WindowsLocalCommandExecutor.execute, LocalComputationManager.execute, ParallelLoadFlowActionSimulator.run, ActionSimulatorTool.run, AmplModelRunner.run, or AmplModelRunner.runAsync can break out of the intended command and execute arbitrary shell commands as the JVM user. The affected itools paths include action-simulator with task-count, security-analysis with external, and dynamic-security-analysis. Downstream CLI tools, libraries, REST front ends, and multi-tenant grid-analysis services that forward less-trusted contingency identifiers or computation parameters into these	N/A	More Details

	APIs can expose the injection remotely. This issue is fixed in version 7.2.2.		
CVE-2026-15973	LimeSurvey Community Edition 7.0.5 contains a stored cross-site scripting vulnerability in the Survey Menu Entries administration page. An authenticated user with the global settings:read permission can create a survey menu entry containing attacker-controlled data. The value is stored in the surveymenu_entries.data field and later inserted into a single-quoted HTML title attribute without context-appropriate encoding. This issue affects LimeSurvey: 7.0.5.	N/A	More Details
CVE-2026-66003	Frappe is a full-stack web application framework written in Python and JavaScript. Prior to version 15.115.0, an access control bypass in the REST API allows a user to read data from Linked DocTypes that they are not authorized to access. When a document references another document through a Link field, the framework does not consistently enforce the linked DocType's own permissions when the record is retrieved through the REST API, so a low-privileged authenticated user can obtain fields from linked records outside their permitted scope. This issue is fixed in version 15.115.0.	N/A	More Details
CVE-2026-54245	Fleet is an open-source device management platform built on osquery. In versions prior to 4.86.2, the Okta conditional access integration in Fleet Premium is vulnerable to SQL injection through a host-supplied value that is used in a database query without proper parameterization, allowing an attacker who controls a single enrolled host to read or modify arbitrary data in the Fleet database. The value is reported by the host's own agent and stored verbatim, then used on an unauthenticated request path that supports the conditional access integration, so any party controlling one enrolled host, the lowest-privilege position in the product, can influence the query. By disclosing arbitrary database contents an attacker can extract stored session tokens and replay them to act as a global administrator, and on a managed fleet that administrator access enables running scripts on enrolled hosts, leading to remote code execution. The issue requires Fleet Premium with the Okta conditional access integration enabled and does not affect instances where it is not configured. This issue is fixed in version 4.86.2.	N/A	More Details
CVE-2026-26445	stomper 5e2741e is vulnerable to Denial of Service. A malicious client can send partial STOMP frames and keep the TCP connections open, which, combined with the broker s use of edge-triggered epoll (EPOLLET) and MSG_PEEK in recv(), causes sockets to enter a permanent half-read state. When enough such connections accumulate, the broker stops receiving any further epoll events for those sockets and eventually hangs in epoll_wait, effectively refusing to process new messages.	N/A	More Details
CVE-2026-22056	StorageGRID (formerly StorageGRID Webscale) versions 11.5 and higher in a non-standard configuration and scenario are susceptible to a Denial of Service vulnerability. Successful exploit could allow an attacker with some control over the environment to cause a partial Denial of Service.	N/A	More Details
CVE-2026-55678	Arc is an open, SQL-native time-series database for telemetry. From 26.02.1 until 26.06.2, Arc Enterprise clustering accepts cluster join requests without authentication when cluster.enabled is true but cluster.shared_secret is not configured. The defaults in internal/config/config.go set cluster.enabled to false, cluster.cluster_name to arc-cluster, cluster.coordinator_addr to :9100, cluster.shared_secret to an empty value, and cluster.tls_enabled to false, while cmd/arc/main.go requires cluster.shared_secret only when cluster.replication_enabled is true. JoinRequest in internal/cluster/protocol/messages.go accepts attacker-controlled node_id, role, raft_addr, api_addr, and coord_addr values, plus optional auth_nonce, auth_timestamp, and auth_hmac fields. The join path in internal/cluster/coordinator.go validates HMAC authentication only when the configured shared secret is non-empty and otherwise proceeds after only the cluster-name check. An accepted node is marked healthy, added as a Raft voter or registered locally, and becomes available through internal/cluster/registry.go to the routing logic in internal/cluster/router.go. The forwardRequest path in internal/cluster/router.go builds its target from node.APIAddress and copies Authorization and x-api-key headers with the request, so a rogue node selected for a forwarded query or write can receive authentication headers, request bodies, database and measurement names, and operational metadata. Heartbeat in internal/cluster/protocol/messages.go also lacks HMAC fields, and internal/cluster/coordinator.go updates node state from supplied node_id and state values without authentication. An unauthenticated network attacker who can reach the coordinator port and knows the cluster name can therefore become a trusted cluster node, mutate cluster membership, be submitted as a Raft voter, intercept topology-dependent forwarded requests, divert or forge operations, and blackhole or delay traffic. The default standalone configuration is not reachable because cluster.enabled is false, but Enterprise cluster deployments with clustering enabled and no shared secret are affected. This issue is fixed in version 26.06.2.	N/A	More Details
CVE-2026-55763	Klever-Go is the Go implementation of the Klever blockchain protocol. Prior to 1.7.19, processPercentageRoyaltiesTransfer in core/kapp/accounts/accounts.go calls SubFromBalance after the split loop and after the royaltiesToPay <= 0 early return. computeSplitRoyalties rejects only when splitToPay > royaltiesToPay, so a valid PercentTransferPercentage = 10000 split consumes exactly 100 percent of the royalty pool, sets royaltiesToPay to zero, and returns before the source account is debited. The split recipient receives the full royaltyAmount while the sender pays nothing and the supply counter is not updated, allowing unbounded off-the-books inflation of the transferred KDA. A KDA owner must configure a TransferPercentage royalty with a 100 percent split, after which any holder's transfer of the asset triggers the mint; the sibling processFixedRoyaltiesTransfer path is not affected because it debits the source before distribution. This issue is fixed in version 1.7.19.	N/A	More Details
CVE-2026-	A NULL pointer dereference vulnerability exists in TL-WR841N v14 in the UPnP service when processing SOAP action requests. A specially crafted SOAP action request containing unexpected XML content may	N/A	More

76649	cause the UPnP daemon to terminate unexpectedly. Successful exploitation may result in a denial-of-service condition affecting UPnP functionality until the service is restarted or the device is rebooted.		Details
CVE-2026-75758	Uncontrolled Recursion vulnerability in the Elixir standard library allows an attacker who controls a list passed to inspect/1, List.to_string/1, or List.to_charlist/1 to exhaust a BEAM node's memory. Inspect.List's charlist branch in lib/elixir/lib/inspect.ex classifies a list as a charlist using List.ascii_printable?/2, which examines only the first :printable_limit (4096 by default) elements, and then calls IO.chardata_to_string/1 on the whole term. A list whose printable prefix exceeds that limit but which contains a later element that is not a code point (an atom, an out-of-range integer, or an improper tail) is therefore mis-classified, and the conversion raises ArgumentError. That conversion runs inside List.to_string/1, whose rescue clause builds its message by interpolating inspect(list), which re-enters the same branch and raises again. The nested inspection is an argument to raise, so the recursion is not in tail position and every level is retained: the process stack grows monotonically while each cycle re-walks the list, until the process is killed by max_heap_size or, by default, the node runs out of memory. List.to_charlist/1 has the same rescue shape. Below the printable limit the inner inspect/1 sees the invalid element within its counter and renders the list in ordinary bracket form, so a single ArgumentError is raised and no recursion occurs. This issue affects elixir: from 1.15.0-rc.0 before 1.18.5, from 1.19.0-rc.0 before 1.19.6, and from 1.20.0-rc.0 before 1.20.4.	N/A	More Details
CVE-2026-76650	A NULL pointer dereference vulnerability exists in TL-WR841N v14 in the UPnP service when processing SOAP state variable query requests. A specially crafted SOAP query may trigger unexpected termination or instability of the process hosting the UPnP service. Successful exploitation may result in a denial-of-service condition affecting UPnP discovery, state query, or related management functionality until the affected process is restarted or the device is rebooted.	N/A	More Details
CVE-2026-76651	A buffer overflow vulnerability exists in the embedded HTTP service in TL-WR841N v14 when processing multipart/form-data requests. Insufficient validation of an attacker-controlled boundary parameter may allow a remote unauthenticated attacker to submit a crafted request that corrupts memory by overwriting data beyond the bounds of an internal buffer. Successful exploitation may result in modification or corruption of process memory, potentially leading to undefined application behavior. Arbitrary code execution, information disclosure, and denial-of-service conditions have not been demonstrated.	N/A	More Details
CVE-2026-19485	A Predictable Resource Name vulnerability in BigQuery Import Staging in Google Cloud Vertex AI Search for Commerce versions prior to 2026-04-27 on Google Cloud Platform allows an attacker knowing the victim's project number to obtain read/write access to staged data and error logs using predictable bucket names. This vulnerability was patched and no customer action is needed.	N/A	More Details
CVE-2026-76784	Multiple TP-Link Kasa smart home devices contain insufficient cryptographic protections in the local device communication protocol. An adjacent network attacker may intercept, replay or forge locally exchanged control messages, potentially resulting in unauthorized device control. Successful exploitation could allow an attacker to manipulate the operational state of an affected device, resulting in unauthorized state changes, disruption of normal device functionality or a denial-of-service condition.	N/A	More Details
CVE-2026-80153	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-35445	Winter CMS is a content management system built on the Laravel PHP framework. In versions prior to 1.2.13, the backend did not validate the handler name submitted through the form postback _handler POST field, allowing an authenticated backend user to invoke arbitrary controller methods, including protected, private, and action-prefixed ones. While AJAX requests validate that handler names match the on[A-Z][\w+]* pattern, the postback path passed the submitted _handler value straight to the handler dispatcher with no such check, so any controller that exposes a public action or conditionally relaxes its $requiredPermissions check could be reached, bypassing the roles and permissions system. The built-in Users controller was affected because it set $requiredPermissions to null for the myaccount action, letting any authenticated backend user invoke user-management methods such as update_onDelete and update_onManualPasswordReset without holding the backend.manage_users permission. This issue is fixed in version 1.2.13.	N/A	More Details
CVE-2026-55764	Klever-Go is the Go implementation of the Klever blockchain protocol. Prior to 1.7.19, Klever-Go allows a mint-role holder to bypass a finite per-nonce MaxSupply on the semi-fungible token add-quantity path. In core/kapp/systemAccount/systemAcount.go, SFTAddCirculation performed meta.Circulation += amount before evaluating whether Circulation exceeded MaxSupply, without checking for signed int64 overflow. A large positive raw Amount supplied through processSemiFungibleAddQuantity in core/kapp/kda/mint.go can wrap Circulation negative, causing the signed maximum-supply comparison to pass and crediting approximately MaxInt64 units while corrupting the on-chain counter. The fungible path is not affected because its MintedValue <= 0 guard detects the overflow. The correction uses the consensus activation flag FixMarketBuyOverflow. This issue is fixed in version 1.7.19.	N/A	More Details
CVE-2026-55867	Graylog is a free and open log management platform. From 6.2.0 until 6.3.12, 7.0.7, and 7.1.2, the DELETE /users/{userId}/tokens/{idOrToken} endpoint implemented by UsersResource.revokeToken() in graylog2-server/src/main/java/org/graylog2/rest/resources/users/UsersResource.java checks USERS_TOKENREMOVE permission against the attacker-controlled userId path parameter before resolving the token selected by idOrToken. An authenticated user can provide an authorized userId while accessTokenService.loadById() or accessTokenService.load() resolves a token belonging to another user, including a service account or administrator, after which accessTokenService.destroy() deletes that token without checking	N/A	More Details

	AccessToken.getUserName(). The issue does not expose token contents, but unauthorized deletion causes integrity impact and can disrupt access-token-based integrations. This issue is fixed in versions 6.3.12, 7.0.7, and 7.1.2.		
CVE-2026-10522	The MemberHero WordPress plugin through 6.9 does not restrict which account fields can be supplied during its frontend registration process, allowing unauthenticated attackers to register a new user with an arbitrary role, including Administrator, leading to a full site takeover. Version 6.9 is advertised as resolving this issue, but the fix is incomplete and the current version remains exploitable by unauthenticated attackers to obtain administrator access and to take over existing accounts. No version that fully addresses the issue is available at the time of this advisory. Mitigation: deactivate and remove the MemberHero WordPress plugin through 6.9 until a version that fully resolves this issue is released. If the MemberHero WordPress plugin through 6.9 must stay active, disable public registration, restrict access to the registration functionality, and monitor the site for unexpected administrator accounts.	N/A	More Details
CVE-2026-55509	WsgiDAV is a generic and extendable WebDAV server based on WSGI. Prior to 4.3.5, the sample MySQLBrowserProvider in wsgidav/samples/mysql_dav_provider.py concatenates the record key parsed from a request URL directly into SQL WHERE clauses. The affected _exists_record_by_primary_key, _get_field_by_primary_key, and _get_record_by_primary_key methods are part of a shipped example provider that is not enabled by default. An attacker who can access a share explicitly configured with this non-default provider can inject SQL through a normal GET request; anonymously exposed read shares permit a status-code oracle and extraction of arbitrary data reachable by the configured MySQL account. This issue is fixed in version 4.3.5.	N/A	More Details
CVE-2026-79921	amqp091-go is a Go AMQP 0.9.1 client. Before version 1.13.0, a compromised or malicious AMQP broker can force the client to allocate resources for and process content body frames that exceed the negotiated frame_max limit. This can lead to unexpected memory consumption or application-layer denial of service (DoS), bypassing the protocol's built-in framing constraints. Version 1.13.0 contains a fix. No known workarounds are available.	N/A	More Details
CVE-2026-55378	JS Recon is a JavaScript enumeration and SAST tool. From 1.2.1-beta.1 until 1.3.1-beta.2, the PR Branch Checker workflow in .github/workflows/pr_checker.yml places github.head_ref and github.event.pull_request.head.repo.full_name into BRANCH_NAME and SOURCE_REPO and interpolates those untrusted values into a shell gh pr comment command. A remote user who opens a pull request can use shell metacharacters in a branch or fork name to execute commands in the GitHub Actions runner with the workflow's GITHUB_TOKEN, which has pull-requests write permission. This issue is fixed in version 1.3.1-beta.2.	N/A	More Details
CVE-2026-55245	Bifrost is an enterprise AI gateway for routing requests to model providers. Prior to 1.5.17, the isPublicIP function in core/providers/utils/fetch.go, reached through FetchAndEncodeURL for Bedrock and Vertex image or document URLs, classifies Carrier-Grade NAT 100.64.0.0/10, IPv6 6to4 2002::/16, NAT64 64:ff9b::/96 and 64:ff9b:1::/48, and deprecated IPv6 site-local fec0::/10 addresses as public. A remote attacker who controls a multimodal request URL can make the gateway fetch internal services, including a cloud instance metadata endpoint encoded through 6to4 or NAT64. This issue is fixed in version 1.5.17.	N/A	More Details
CVE-2026-51611	Incorrect access control in the startSlaveReboot function of TOTOLINK T6 4.1.5cu.748_B20211015 allows unauthenticated attackers to arbitrarily force a reboot via sending a crafted MQTT message.	N/A	More Details
CVE-2023-46702	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is Unused	N/A	More Details
CVE-2026-69129	KubePi is a Kubernetes multi-cluster management panel. In versions up to and including 2.0.0, cluster-scoped APIs do not consistently validate per-cluster access, allowing an authenticated user with cluster management permissions to operate on clusters outside the scope they were granted. Because the affected endpoints act on cluster-specific data without confirming that the requesting user is authorized for that particular cluster, a user assigned management rights over one cluster can, under certain role and cluster configurations, read or modify data in clusters they should not manage. This issue is fixed in version 2.0.1.	N/A	More Details
CVE-2026-65956	KubePi is a Kubernetes multi-cluster management panel. In versions up to and including 1.6.15, the SSO configuration API endpoints are exposed on the same public routing boundary as the SSO login and callback endpoints, so SSO, OIDC, and SAML management operations can be reached without administrator authorization. Because reading, creating, and updating the global SSO configuration is not restricted to administrators, an unauthorized or low-privileged user can inspect or alter the authentication configuration, which under certain conditions can lead to account takeover or privilege escalation. The SSO connectivity-test function can additionally be abused as a server-side request forgery primitive, and the user list API returns user objects without consistently clearing authentication-related fields. This issue is fixed in version 2.0.0.	N/A	More Details
CVE-2026-18823	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-	SeaweedFS is a distributed storage system for files and blobs. In versions 4.39 and earlier, the S3 API accepts an external OIDC JWT sent directly in the Authorization header and maps it to an IAM role without enforcing that role's trust policy, so a federated user can assume a role they are not permitted to hold. The standard STS AssumeRoleWithWebIdentity path rejects such a token when the role's trust policy does not		More

77298	trust the token's federated provider, but the direct S3 bearer path validates only the token itself and then authenticates as the mapped role and evaluates that role's attached S3 permissions. As a result, a valid OIDC user whose token would be denied the role through STS can obtain the role's S3 access, including object read, write, and delete, by presenting the raw OIDC JWT directly to the S3 API. This issue is fixed in version 4.40	N/A	Details
CVE-2026-65930	LimeSurvey Community Edition 7.0.5 contains an authenticated stored cross-site scripting vulnerability in the replacement-fields dialog used by the administrative question editor.This issue affects LimeSurvey: 7.0.5.	N/A	More Details
CVE-2026-65647	Improper symlink resolution before file access in Plesk allows remote authenticated users to execute arbitrary code as root.	N/A	More Details
CVE-2026-65646	Improper neutralization of special elements in Plesk allows remote authenticated users to disclose arbitrary local files and escalate privileges.	N/A	More Details
CVE-2026-65642	Insecure direct object reference in Plesk 18.0.79.7 and earlier or 18.0.80 through 18.0.80.3, allows remote authenticated users to read and modify other customers' databases.	N/A	More Details
CVE-2026-65641	A vulnerability allowing an unauthenticated network attacker to coerce SMB authentication from the service account.	N/A	More Details
CVE-2026-64632	A vulnerability allowing a low-privileged user to capture the NTLM credentials of the Reporter service account.	N/A	More Details
CVE-2026-63360	LimeSurvey Community Edition 7.0.5+260623 contains an authenticated reflected Cross-Site Scripting vulnerability in the user activation confirmation endpoint. The action query parameter is copied into the response and inserted into a hidden input attribute without HTML attribute encoding. This issue affects LimeSurvey: 7.0.5.	N/A	More Details
CVE-2026-58070	A vulnerability that records guest OS processing credentials in cleartext in a support log on the guest, allowing a user with read access to that log to recover privileged account credentials.	N/A	More Details
CVE-2026-54766	Vikunja is an open-source self-hosted task management platform. From 0.21.0 until 2.4.0, the project duplication operation in pkg/models/project_duplicate.go allows an authenticated user who can read a source project to place its duplicate beneath an arbitrary target parent project. ProjectDuplicate.CanCreate calls parent.CanCreate on an unhydrated Project containing only the body supplied parent_project_id instead of calling parent.CanWrite, so the target parent write-permission check is skipped. The ordinary project creation path enforces that permission, but PUT /api/v1/projects/{project}/duplicate does not, allowing attacker-owned content to be injected into another user or team project hierarchy. This issue is fixed in version 2.4.0.	N/A	More Details
CVE-2026-55182	LibreNMS is a network monitoring system. In versions from 21.6.0 up to 26.5.0, the Signal alert transport is vulnerable to command injection because the signal-cli path and the Recipient field of an alert transport entry are insufficiently escaped before being passed to an exec call. An authenticated administrator can craft a transport entry whose Recipient contains shell metacharacters and whose path points to the bundled composer_wrapper.php script, which itself passes attacker-controlled input to further unsafe exec calls. By chaining these calls, the administrator can execute arbitrary operating-system commands on the LibreNMS host. This issue is fixed in version 26.5.0.	N/A	More Details
CVE-2026-55068	free5GC is an open-source implementation of the 5G core network. In 4.2.2 and earlier, the NRF RegisterNFInstance handler at PUT /nnrf-nfm/v1/nf-instances/{nfInstanceID} accepts NF Profiles without enforcing UUID format, nfStatus enum values, heartBeatTimer ranges, mandatory profile fields, or nfServices.ipEndPoints address constraints. The invalid profiles are persisted in the MongoDB NfProfile collection and returned by NFDiscover, allowing an attacker with SBI access to advertise attacker-controlled network-function endpoints and redirect control-plane signaling. This can expose credentials and signaling, alter service discovery integrity, and deny service across network functions that trust the NRF. This issue is fixed in version 4.2.3.	N/A	More Details
CVE-2026-16809	LimeSurvey Community Edition 7.0.5 contains a stored cross-site scripting vulnerability in the survey quota creation workflow. An authenticated low-privileged user who can create and manage their own survey can store malicious JavaScript in a quota message. This issue affects LimeSurvey: 7.0.5.	N/A	More Details
CVE-2026-55220	Pimcore is an Open Source Data & Experience Management Platform. Prior to 11.5.19, 12.3.10, and 2026.1.6, Pimcore\Model\DataObject\ClassDefinition\Data\Hotspotimage::getDataFromResource() in models/DataObject/ClassDefinition/Data/Hotspotimage.php passes the field __hotspots object-store column to Pimcore\Tool\Serialize::unserialize() without an allowed-classes restriction after JSON decoding fails. An attacker with a separate capability to write crafted PHP serialized bytes into that column can instantiate available classes and trigger magic methods when an affected DataObject is loaded, which can produce arbitrary file writes or code execution through bundled gadget chains. The related ImageGallery, Block, and Video callers use the same fallback pattern, but the identified June fix changes the Hotspotimage caller only. This issue is fixed for Hotspotimage in versions 11.5.19, 12.3.10, and 2026.1.6.	N/A	More Details
CVE-2026-77989	Joomla Extension - joomlaeventmanager.net - Reflected XSS via the PDF export link in Joomla Events Manager < 5.0.1 - buildCurrentPdfLink copies the current request query string into the PDF button URL, and	N/A	More Details

	pdfbutton() echoes it unescaped, leading to an reflected XSS vector.		
CVE-2026-80690	In the Linux kernel, the following vulnerability has been resolved: scsi: ufs: core: Initialize hba->rpmbs list in ufshcd Initialize the hba->rpmbs list in ufshcd_alloc_host() to prevent NULL pointer dereference in the device teardown path if ufs_rpmb_probe() fails.	N/A	More Details
CVE-2026-80689	In the Linux kernel, the following vulnerability has been resolved: tracing/mmiotrace: Add NULL check for mmio_trace_array in logging functions mmio_trace_rw() and mmio_trace_mapping() retrieve mmio_trace_array into tr and pass it to __trace_mmiotrace_rw() and __trace_mmiotrace_map(). If these functions are invoked while mmio_trace_array is NULL (e.g. before initialization or after disabled), accessing tr->array_buffer.buffer will result in a NULL pointer dereference crash. Fix this by adding an explicit NULL check for tr at the beginning of __trace_mmiotrace_rw() and __trace_mmiotrace_map().	N/A	More Details
CVE-2026-80595	In the Linux kernel, the following vulnerability has been resolved: Input: ims-pcu - add response length checks The driver processes response data from device buffers without verifying that the device actually sent enough data. This can lead to out-of-bounds reads or processing stale data. Add checks for the expected response length before accessing the buffers.	N/A	More Details
CVE-2026-77838	SOY Calendar contains a cross-site scripting vulnerability. An arbitrary script may be executed on the web browser of the user who is logging in to the product.	N/A	More Details
CVE-2026-78032	SOY CMS contains an issue with deserialization of untrusted data. An arbitrary code may be executed by an attacker with the web server privilege.	N/A	More Details
CVE-2026-78238	SOY Gallery contains a cross-site scripting vulnerability. An arbitrary script may be executed on the web browser of the user who is logging in to the product.	N/A	More Details
CVE-2021-48002	Rejected reason: This CVE ID has been rejected.	N/A	More Details
CVE-2021-48001	Rejected reason: This CVE ID has been rejected.	N/A	More Details
CVE-2021-48000	Rejected reason: This CVE ID has been rejected.	N/A	More Details
CVE-2026-80592	In the Linux kernel, the following vulnerability has been resolved: samples/damon/mtier: fail early if address range parameters are invalid The comment on top of `struct damon_region` clearly says that For any use case, @ar should be non-zero positive size. which is now verified in damon_verify_new_region() if the kernel is built with DAMON_DEBUG_SANITY. The WARN_ONCE() can be triggered if the mtier sample module is enabled before node{0,1}_{start,end}_addr have been properly initialized, which is obviously not good. ----------[cut here]---------- start 0 >= end 0 WARNING: mm/damon/core.c:217 at damon_new_region+0xf4/0x118, CPU#59: bash/341468 Call trace: damon_new_region+0xf4/0x118 (P) damon_set_regions+0xfc/0x3c0 damon_sample_mtier_build_ctx+0xe8/0x3a8 damon_sample_mtier_start+0x1c/0x90 damon_sample_mtier_enable_store+0x98/0xb0 param_attr_store+0xb4/0x128 module_attr_store+0x2c/0x50 sysfs_kf_write+0x58/0x90 kernfs_fop_write_iter+0x16c/0x238 vfs_write+0x2c0/0x370 ksys_write+0x74/0x118 __arm64_sys_write+0x24/0x38 invoke_syscall+0xa8/0x118 el0_svc_common.constprop.0+0x48/0xf0 do_el0_svc+0x24/0x38 el0_svc+0x54/0x370 el0t_64_sync_handler+0xa0/0xe8 el0t_64_sync+0x1ac/0x1b0 ---[end trace 0000000000000000]--- Note that the same issue can happen if detect_node_addresses is true, and node 0 or 1 is memoryless. Fix it together by checking the validity of parameters right before damon_new_region() and fail early if they're invalid.	N/A	More Details
CVE-2021-47999	Rejected reason: This CVE ID has been rejected.	N/A	More Details
CVE-2026-80594	In the Linux kernel, the following vulnerability has been resolved: Input: ims-pcu - fix potential infinite loop in CDC union descriptor parsing The driver parses CDC union descriptors in ims_pcu_get_cdc_union_desc() by iterating through the extra descriptor data. However, it does not verify that the bLength of each descriptor is at least 2. A malicious device could provide a descriptor with bLength = 0, leading to an infinite loop in the driver. Add a check to ensure bLength is at least 2 before proceeding with parsing.	N/A	More Details
CVE-2021-47998	Rejected reason: This CVE ID has been rejected.	N/A	More Details
CVE-2026-80610	In the Linux kernel, the following vulnerability has been resolved: net: enetc: fix potential divide-by-zero when num_vsi is zero For i.MX94 series, all the standalone ENETCs do not support SR-IOV, so pf->caps.num_vsi is zero. This leads to a divide-by-zero in enetc4_default_rings_allocation() when distributing rings among PF and VFs. Division by zero is undefined behavior in C. On ARM64, the UDIV/SDIV instructions silently return zero rather than raising an exception, so the issue does not cause a visible crash. However, relying on this behavior is incorrect and poses a cross-platform compatibility risk. Add an explicit check for num_vsi == 0 and return early after the PF's rings have been configured.	N/A	More Details
CVE-2026-80597	In the Linux kernel, the following vulnerability has been resolved: mtd: maps: vmu-flash: fix NULL pointer dereference in initialization The mtd_info contains a struct device, which must be linked to its parent.	N/A	More Details

	Without this, the initialization of the MTD fails with a NULL pointer dereference.		
CVE-2021-47997	Rejected reason: This CVE ID has been rejected.	N/A	More Details
CVE-2026-81814	Affected versions of Flowintel render calendar event titles using innerHTML. Because those titles are derived from case titles, a user able to create or modify a case title could store HTML or script-capable content that is later interpreted by the browser when another user views the calendar. The fix changes: titleEl.innerHTML = arg.event.title to: titleEl.textContent = arg.event.title || '' and similarly stops using innerHTML for the static download icon. Version impacted =>3.3.0	N/A	More Details
CVE-2026-81753	Affected versions of Flowintel render Mermaid blocks contained in stored case notes without sufficiently neutralizing attacker-controlled markup. Because Mermaid note content is persisted and later rendered for other users, an attacker with permission to create or edit a note could store a crafted Mermaid payload that results in JavaScript execution when another user views the affected case note. The patch adds explicit Mermaid detection and HTML escaping around the token content before the generated Mermaid wrapper is returned. It also moves the wrapping logic earlier in page initialization so Markdown instances are protected consistently. Version impacted >= 3.3.0	N/A	More Details
CVE-2026-80602	In the Linux kernel, the following vulnerability has been resolved: perf/x86/amd/lbr: Fix kernel address leakage A user-only branch stack can contain branches that originate from the kernel. As a result, kernel addresses are exposed to user space even when PERF_SAMPLE_BRANCH_USER is requested. On AMD processors supporting X86_FEATURE_AMD_LBR_V2, perf can still report SYSRET/ERET entries for which the branch-from addresses are in the kernel. E.g. $ perf record -e cycles -o - -j any,save_type,u -- \ perf bench syscall basic --loop 1000 | \ perf script -i - -F brstack|tr ' ' '\n'| \ grep -E '0x[89a-f][0-9a-f]{15}' ... 0xffffffff81001268/0x717a90a38f1a/M/-/-/0/ERET/NON_SPEC_CORRECT_PATH 0xffffffff81001268/0x717a90a39157/M/-/-/0/ERET/NON_SPEC_CORRECT_PATH 0xffffffff81001268/0x717a90a2c628/M/-/-/0/ERET/NON_SPEC_CORRECT_PATH 0xffffffff81001268/0x717a90a41b60/M/-/-/0/ERET/NON_SPEC_CORRECT_PATH 0xffffffff81001268/0x717a90a260db/M/-/-/0/ERET/NON_SPEC_CORRECT_PATH 0xffffffff81001268/0x717a90a260db/M/-/-/0/ERET/NON_SPEC_CORRECT_PATH 0xffffffff81001268/0x717a8bef1c30/M/-/-/0/ERET/NON_SPEC_CORRECT_PATH 0xffffffff81001268/0x717a8e4d3c90/M/-/-/0/ERET/NON_SPEC_CORRECT_PATH ... The reason is that the hardware filter only considers the privilege level applicable to the branch target. Extend software filtering to also validate the branch-from addresses against br_sel, so that any branch record whose branch-from address is in the kernel is dropped when PERF_SAMPLE_BRANCH_USER is requested.	N/A	More Details
CVE-2026-81743	Affected versions of Flowintel allow the LOG_FILE configuration value to be modified through system settings without restricting it to a filename inside the intended log directory. Because the application constructs the log destination from this configurable value, an administrator could set LOG_FILE to an arbitrary filesystem path. Since attackers can influence logged content, this enables controlled data to be written into unintended files. The upstream commit specifically describes an exploitation chain in which an attacker injects a template into a chosen file and subsequently abuses application rendering behavior to execute code. The patch removes LOG_FILE from the web-editable settings, introduces validate_log_file_name() to reject absolute paths, traversal, Windows paths, null bytes, and directory components, and centralizes log path construction through resolve_log_file_path(). Version impacted: >=3.3.0	N/A	More Details
CVE-2026-80605	In the Linux kernel, the following vulnerability has been resolved: HID: picolcd: prevent NULL pointer dereference in picolcd_send_and_wait() In picolcd_send_and_wait(), an integer overflow of the signed loop counter 'k' can theoretically lead to a NULL pointer dereference of 'raw_data'. If the loop executes more than INT_MAX times, 'k' becomes negative, making the condition 'k < size' true even when 'size' is 0. Change the type of 'k' to 'unsigned int' to prevent the overflow and eliminate the out-of-bounds access. Found by Linux Verification Center (linuxtesting.org) with the Svace static analysis tool. [jkosina@suse.com: extended hash length]	N/A	More Details
CVE-2026-81677	The ‘/ws/apiprensa/getVideo’ endpoint is vulnerable to SQL injection due to improper validation of the GET parameter `id_ambito`. An attacker can inject SQL syntax that breaks the underlying structure of the MariaDB query, resulting in syntax errors and the exposure of database error messages via PDOException. This confirms that user input is being incorporated directly into SQL statements without proper sanitization or the use of prepared statements.	N/A	More Details
CVE-2026-80607	In the Linux kernel, the following vulnerability has been resolved: tracing/probes: Remove WARN_ON_ONCE from parse_btf_arg Sashiko found that user can cause this WARN_ON_ONCE() easily with adding a kprobe event based on a raw address with BTF parameter. Since this is not an unexpected condition, remove the WARN_ON_ONCE().	N/A	More Details
CVE-2026-73827	SOY Calendar contains a cross-site scripting vulnerability. An arbitrary script may be executed on the web browser of the user who is logging in to the product.	N/A	More Details
CVE-2021-48003	Rejected reason: This CVE ID has been rejected.	N/A	More Details
CVE-2021-	Rejected reason: This CVE ID has been rejected.	N/A	More

48004			Details
CVE-2021-48005	Rejected reason: This CVE ID has been rejected.	N/A	More Details
CVE-2026-78499	A server-side request forgery (SSRF) vulnerability WatchGuard Dimension FTP Server Test configuration allows an authenticated privileged attacker to enumerate exposed network services on adjacent network systems.	N/A	More Details
CVE-2026-78500	A blind server-side request forgery (SSRF) vulnerability WatchGuard Dimension Database Server Test configuration allows an authenticated privileged attacker to enumerate exposed network services on adjacent network systems.	N/A	More Details
CVE-2026-78610	WatchGuard Dimension's Web UI exposes an administrator passphrase change action that lacks CSRF protection. An attacker who can induce an authenticated global administrator's browser to visit a crafted link or page can change that administrator's passphrase to an attacker-chosen value without the administrator's consent.	N/A	More Details
CVE-2026-78612	WatchGuard Dimension contains an authenticated SQL injection vulnerability in the scheduled report feature which allows an authenticated user with report administration permissions gain arbitrary command execution as the Dimension WebUI process user by sending specially crafted requests.	N/A	More Details
CVE-2026-78613	WatchGuard Dimension contains an authenticated SQL injection vulnerability in the log viewer feature which allows an authenticated user with report administration permissions gain arbitrary command execution as the Dimension WebUI process user by sending specially crafted requests.	N/A	More Details
CVE-2026-78614	WatchGuard Dimension contains an authenticated SQL injection vulnerability in the audit report feature which allows an authenticated user with report administration permissions gain arbitrary command execution as the Dimension WebUI process user by sending specially crafted requests.	N/A	More Details
CVE-2026-78615	A Reflected Cross-Site Scripting (XSS) vulnerability in WatchGuard Dimension's report detail page allows an attacker to execute arbitrary JavaScript in a authenticated user's browser with a specially crafted URL.	N/A	More Details
CVE-2026-78616	A Stored Cross-Site Scripting (XSS) vulnerability in WatchGuard Dimension's Trusted CA certificate configuration allows an authenticated administrator to execute arbitrary JavaScript in another authenticated administrator's web browser by saving a carefully crafted certificate.	N/A	More Details
CVE-2026-78617	WatchGuard Dimension's web login endpoint does not enforce effective rate-limiting or account lockout by default allowing a remote attacker to perform automated password guessing against user accounts. If the account lockout setting is enabled, brute-force attempts are blocked after a defined number of failed attempts, but this setting is not enabled by default.	N/A	More Details
CVE-2026-78618	A business logic flaw in WatchGuard Dimension allows an authenticated administrator to trigger multiple backend operations within a single logical flow by sending a specially crafted request.	N/A	More Details
CVE-2022-51007	Rejected reason: This CVE ID has been rejected.	N/A	More Details
CVE-2022-51006	Rejected reason: This CVE ID has been rejected.	N/A	More Details
CVE-2022-51005	Rejected reason: This CVE ID has been rejected.	N/A	More Details
CVE-2022-51004	Rejected reason: This CVE ID has been rejected.	N/A	More Details
CVE-2022-51003	Rejected reason: This CVE ID has been rejected.	N/A	More Details
CVE-2026-82089	The wallabag (aka fr.gaulupeau.apps.InThePoche) application through 2.6.0 for Android allows XSS because /api/entries data is loaded into a WebView.	N/A	More Details
CVE-2026-82090	Pocket through 8.33.0.0 allows XSS because "Save to Pocket" injects external HTML into the DOM. JavaScript code can alter the application state via native bridge methods.	N/A	More Details
CVE-2022-51002	Rejected reason: This CVE ID has been rejected.	N/A	More Details
CVE-2022-51001	Rejected reason: This CVE ID has been rejected.	N/A	More Details
CVE-2026-81676	A vulnerability in the endpoint ‘/ws/apitribuna/ultimosVideos’ where the `limit_videos` parameter is directly concatenated into a MariaDB SQL query without proper sanitization or parameterization. By injecting SQL syntax into this parameter, a remote attacker can cause SQL syntax errors and potentially manipulate backend queries. The issue results in an error-based SQL injection and exposes internal database error	N/A	More Details

	messages and stack traces, revealing implementation details of the backend system.		
CVE-2026-80611	In the Linux kernel, the following vulnerability has been resolved: ACPI: processor_idle: Mark LPI enter functions as __cpuidle When function tracing or Kprobes is enabled, entering an ACPI Low Power Idle (LPI) state triggers the following RCU splat: RCU not on for: acpi_idle_lpi_enter+0x4/0xd8 WARNING: CPU: 8 PID: 0 at include/linux/trace_recursion.h:162 function_trace_call+0x1e8/0x228 The acpi_idle_lpi_enter() function is invoked within the cpuidle path after RCU has already been disabled for the current local CPU. Consequently, ftrace's function_trace_call() expects RCU to be actively watching before recording trace data, emitting a warning if it is not. Fix this by annotating acpi_idle_lpi_enter(), the generic __weak stub, and the RISC-V implementation of acpi_processor_ffh_lpi_enter() with __cpuidle. This moves these functions into the '.cpuidle.text' section, implicitly disabling ftrace instrumentation (notrace) along this sensitive path and preventing trace-induced RCU warnings during idle entry.	N/A	More Details
CVE-2026-80688	In the Linux kernel, the following vulnerability has been resolved: riscv: drop __init from vec_check_unaligned_access_speed_all_cpus This function runs within a kthread and need not necessarily finish before system finishes boot and free_initmem() unmaps the .init.text section. This function makes calls to SBI for probing unaligned access speed, and if this is slow for some reason (say some debug prints were added to SBI), the kthread can still be running at this point and result in an instruction page fault when trying to fetch from the freed region. [25.642087] Unable to handle kernel paging request at virtual address ffffffff80a04ef8 [25.646694] Current vec_check_unali pgtable: 4K pagesize, 48-bit VAs, pgdp=0x00004000316e9000 [25.653170] [ffffffff80a04ef8] pgd=000010004be7e401, p4d=000010004be7e401, pud=000010004be7e001, pmd=000010000c3000e3 [25.661244] Oops [#1] [25.662997] Modules linked in: [25.665357] CPU: 3 UID: 0 PID: 42 Comm: vec_check_unali Not tainted 7.0.0-tt-blackhole-asrinivasan-00007-g30ff73f18211 #570 PREEMPTLAZY [25.674669] Hardware name: Tenstorrent Blackhole (DT) [25.678545] epc : vec_check_unaligned_access_speed_all_cpus+0x18/0x2c [25.683458] ra : vec_check_unaligned_access_speed_all_cpus+0x18/0x2c [25.688372] epc : ffffffff80a04ef8 ra : ffffffff80a04ef8 sp : ffff8f8000203e20 [25.693874] gp : ffffffff814dc168 tp : ffffaf8001ad9900 t0 : 0000000000000000 [25.699401] t1 : ffffffffffffffff0 t2 : ffffaf8001ad9a10 s0 : ffff8f8000203e30 [25.704912] s1 : ffffaf80018dc780 a0 : 0000000000000000 a1 : 0000000000000002 [25.710407] a2 : 00000000000001f0 a3 : 0000000000000018 a4 : 0000000000000000 [25.715917] a5 : 0000000000000000 a6 : ffffaf8001c03d98 a7 : ffffaf8001c03e30 [25.721419] s2 : ffff8f8000023c98 s3 : ffffaf8001aa1240 s4 : ffffffff80a04ee0 [25.726937] s5 : 0000000000000000 s6 : 0000000000000000 s7 : 0000000000000000 [25.732450] s8 : 0000000000000000 s9 : 0000000000000000 s10: 0000000000000000 [25.737944] s11: 0000000000000000 t3 : 0000000000000002 t4 : 0000000000000402 [25.743481] t5 : 0000000000000040 t6 : 0000000000000004 ssp : 0000000000000000 [25.749024] status: 0000000200000120 badaddr: ffffffff80a04ef8 cause: 000000000000000c [25.755060] [<ffffffff80a04ef8>] vec_check_unaligned_access_speed_all_cpus+0x18/0x2c [25.760964] [<ffffffff80047a10>] kthread+0xd8/0xfc [25.764660] [<ffffffff80010c48>] ret_from_fork_kernel+0x18/0x1c4 [25.769220] [<ffffffff80895fe6>] ret_from_fork_kernel_asm+0x16/0x18 [25.774018] Code: cccc cccc cccc cccc cccc cccc cccc cccc cccc cccc (cccc) cccc Drop __init from its signature so that this doesn't happen.	N/A	More Details
CVE-2026-80659	In the Linux kernel, the following vulnerability has been resolved: mmc: vub300: defer reset until cmd_mutex is unlocked vub300_cmndwork_thread() holds cmd_mutex while it sends a command and waits for the command response. If the response wait times out, __vub300_command_response() kills the command URBs and then synchronously resets the USB device through usb_reset_device(). That reset path re-enters the driver through vub300_pre_reset(), which also takes cmd_mutex. The worker therefore tries to acquire the same mutex recursively while it is still holding it from the command path. This issue was found by our static analysis tool and then manually reviewed against the current tree. The grounded PoC kept the real worker and timeout/reset carrier: vub300_cmndwork_thread() __vub300_command_response() usb_lock_device_for_reset() usb_reset_device() vub300_pre_reset() Lockdep reported the same-task recursive acquisition on cmd_mutex: WARNING: possible recursive locking detected ... (&test_vub300.cmd_mutex) ... at: usb_reset_device... [vuln_msv] ... (&test_vub300.cmd_mutex) ... at: vub300_cmndwork_thread+0x12/0x20 [vuln_msv] Workqueue: vub300_cmd_wq vub300_cmndwork_thread [vuln_msv] *** DEADLOCK *** Return a flag from __vub300_command_response() when the timeout path needs a device reset, then perform the reset after vub300_cmndwork_thread() has cleared the in-flight command state and dropped cmd_mutex. The reset is still attempted before mmc_request_done(), preserving the existing request completion ordering while avoiding the recursive lock.	N/A	More Details
CVE-2026-80647	In the Linux kernel, the following vulnerability has been resolved: RDMA/hns: Fix warning in poll cq direct mode CQs allocated by ib_alloc_cq() always have a comp_handler. Though in direct mode this handler is never expected to be called, it is still called when the driver is reset, triggering the following WARN_ONCE(): Call trace: ib_cq_completion_direct+0x38/0x60 hns_roce_cq_completion+0x54/0x90 (hns_roce_hw_v2) hns_roce_handle_device_err+Ox1c8/0x340 [hns_roce_hw_v2] hns_roce_hw_v2_uninit_instance.constprop.0+0x34/0x70 [hns_roce_hw_v2] hns_roce_hw_v2_reset_notify+0xc4/0xe0 [hns_roce_hw_v2] hclge_notify_roce_client+0x60/0xbc [hclge] hclge_reset_rebuild+0x48/0x34c [hclge] hclge_reset_subtask+0xcc/0xec [hclge] hclge_reset_service_task+0x80/0x160 [hclge] hclge_service_task+0x50/0x80 (hclge] process_one_work+0x1cc/0x4d0 worker_thread+0x154/0x414 kthread+0x104/0x144 ret_from_fork+0x10/0x18	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: pinctrl: spacemit: fix NULL check in spacemit_pin_set_config spacemit_pin_set_config() looks up the per-pin descriptor with spacemit_get_pin()		

CVE-2026-80648	then checks the wrong variable for failure: const struct spacemit_pin *spin = spacemit_get_pin(pctrl, pin); ... if (!pin) return -EINVAL; reg = spacemit_pin_to_reg(pctrl, spin->pin); pin is an unsigned int pin id, where 0 (GPIO_0 / gmac0_rxdv on K3) is a valid pin, so rejecting it here drops the PAD config write for the first pin of every group. On K3 Pico-ITX the GMAC RGMII group lists pin 0 as its first entry, so its drive-strength / bias configuration was silently ignored. The intended guard is against spacemit_get_pin() returning NULL when the pin id isn't in the SoC's pin table. Check spin instead, which both restores PAD setup for pin 0 and prevents a NULL deref on spin->pin.	N/A	More Details
CVE-2026-80650	In the Linux kernel, the following vulnerability has been resolved: media: atomisp: gc2235: fix UAF and memory leak gc2235_probe() handles its error paths incorrectly. If media_entity_pads_init() fails, gc2235_remove() is called, which tears down the subdev and frees dev, but then still falls through to atomisp_register_i2c_module(). This results in use-after-free. If atomisp_register_i2c_module() fails, the media entity and control handler are left initialized and dev is leaked. gc2235_remove() unconditionally calls media_entity_cleanup() and v4l2_ctrl_handler_free(), but these are not initialized at every error path in gc2235_probe(). Replace gc2235_remove() calls in the probe error paths with explicit unwind labels that free only the resources initialized at each point of failure, in reverse order of initialization.	N/A	More Details
CVE-2026-80651	In the Linux kernel, the following vulnerability has been resolved: crypto: ccp/sev-dev-tsm - bail out early when pdev->bus is NULL dsm_create() initially checks pdev->bus when computing segment_id: u8 segment_id = pdev->bus ? pci_domain_nr(pdev->bus) : 0; But the next two lines unconditionally dereference pdev->bus via pcie_find_root_port() and especially pci_dev_id(pdev), which expands to PCI_DEVID(dev->bus->number, dev->devfn). If pdev->bus is in fact NULL, segment_id is initialised to 0 but the very next statement crashes the kernel. smatch flags this: drivers/crypto/ccp/sev-dev-tsm.c:253 dsm_create() error: we previously assumed 'pdev->bus' could be null (see line 251) Make the NULL handling consistent: if pdev->bus is NULL the device has no PCI context to work with and SEV TIO setup cannot proceed, so return -ENODEV before any of the bus-dependent lookups. The remaining initialisation now runs only on the path where pdev->bus is known to be valid. No change for callers where pdev->bus is non-NULL, which is the only case where dsm_create() did meaningful work before this change.	N/A	More Details
CVE-2026-80652	In the Linux kernel, the following vulnerability has been resolved: crypto: ccp - Treat zero-length cert chain as query for blob lengths When handling a PDH export, treat a zero-length userspace cert chain buffer as a request to query the length of the relevant blobs. Failure to account for the zero-length buffer trips a BUG_ON() when running with CONFIG_DEBUG_VIRTUAL=y due to trying to get the physical address of the ZERO_SIZE_PTR (returned by kzalloc() on the bogus allocation). kernel BUG at arch/x86/mm/physaddr.c:28 ! Oops: invalid opcode: 0000 [#1] SMP KASAN NOPTI CPU: 30 UID: 0 PID: 28580 Comm: syz.2.18 Kdump: loaded Tainted: G W 6.18.16-smp-DEV #1 NONE Tainted: [W]=WARN Hardware name: Google, Inc. Arcadia_IT_80/Arcadia_IT_80, BIOS 12.62.0-0 11/19/2025 RIP: 0010:__phys_addr+0x16a/0x180 arch/x86/mm/physaddr.c:28 RSP: 0018:ffffc9008329fc80 EFLAGS: 00010293 RAX: ffffffff8179110a RBX: 0000778000000010 RCX: ffff8884e6992600 RDX: 0000000000000000 RSI: 0000000080000010 RDI: 0000778000000010 RBP: ffffc9008329fdf0 R08: 0000000000000dc0 R09: 00000000ffffffff R10: dffffc0000000000 R11: fffffbfff126d297 R12: dffffc0000000000 R13: 1ffff92010653fc8 R14: 0000000080000010 R15: dffffc0000000000 FS: 0000555556bec9c0(0000) GS:ffff88aa4ce1c000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007fd3159e7000 CR3: 00000004fbc44000 CR4: 0000000000350ef0 Call Trace: <TASK> [<ffffffff853d3869>] sev_ioctl_do_pdh_export+0x559/0x7a0 drivers/crypto/ccp/sev-dev.c:2308 [<ffffffff853d1fdd>] sev_ioctl+0x2cd/0x480 drivers/crypto/ccp/sev-dev.c:2556 [<ffffffff82549ebc>] vfs_ioctl fs/ioctl.c:52 [inline] [<ffffffff82549ebc>] __do_sys_ioctl fs/ioctl.c:598 [inline] [<ffffffff82549ebc>] __se_sys_ioctl+0xfc/0x170 fs/ioctl.c:584 [<ffffffff8630115f>] do_syscall_x64 arch/x86/entry/syscall_64.c:64 [inline] [<ffffffff8630115f>] do_syscall_64+0x9f/0xf40 arch/x86/entry/syscall_64.c:98 [<ffffffff81000136>] entry_SYSCALL_64_after_hwframe+0x76/0x7e RIP: 0033:0x7fd3158eac39 </TASK> Thankfully, the bug is benign outside of CONFIG_DEBUG_VIRTUAL=y as getting the physical address is just arithmetic, and the PSP errors out before trying to write to the garbage address (which it must, otherwise querying the blob lengths would clobber memory at pfn=0).	N/A	More Details
CVE-2026-80654	In the Linux kernel, the following vulnerability has been resolved: soc: xilinx: Shutdown and free rx mailbox channel A mbox rx channel is requested using mbox_request_channel_byname() in probe. In remove callback, the rx mailbox channel is cleaned up when the rx_chan is NULL due to incorrect condition check. The mailbox channel is not shutdown and it can receive messages even after the device removal. This leads to use after free. Also the channel resources are not freed. Fix this by checking the rx_chan correctly.	N/A	More Details
CVE-2026-80655	In the Linux kernel, the following vulnerability has been resolved: soc: xilinx: Fix race condition in event registration The zynqmp_power driver registers handlers for suspend and subsystem restart events using register_event(). However, the work structures (zynqmp_pm_init_suspend_work and zynqmp_pm_init_restart_work) used by these handlers were allocated and initialized after the registration call. This created a race window where, if the firmware triggered an event immediately after registration but before allocation, the callback (suspend_event_callback or subsystem_restart_event_callback) would dereference a NULL pointer in work_pending(), leading to a crash. Fix this by allocating and initializing the work structures before registering the events.	N/A	More Details
CVE-2026-80657	In the Linux kernel, the following vulnerability has been resolved: accel/amdxdna: Guard management mailbox channel cleanup against NULL pointer The management mailbox channel cleanup helpers can be called from error handling paths when mgmt_chann has already been destroyed. Add NULL checks to xdna_mailbox_free_channel() and xdna_mailbox_stop_channel() so the cleanup path safely returns instead	N/A	More Details

	of dereferencing a NULL mailbox channel pointer.		
CVE-2026-80658	In the Linux kernel, the following vulnerability has been resolved: drm/rockchip: dw_dp: Fix null-ptr-deref in dw_dp_remove() Attempting to access driver data in the platform driver ->remove() callback may lead to a null pointer dereference since there is no guaranty that the component ->bind() callback invoking platform_set_drvdata() was executed. A common scenario is when Rockchip DRM driver didn't manage to run component_bind_all() because of an (unrelated) error causing early return from rockchip_drm_bind(). Drop the unnecessary call to platform_get_drvdata() and, instead, reference the target device structure via platform_device.	N/A	More Details
CVE-2026-80660	In the Linux kernel, the following vulnerability has been resolved: hwmon: (occ) unregister sysfs devices outside occ lock occ_active(false) and occ_shutdown() unregister sysfs-backed devices while occ->lock is held. hwmon_device_unregister() and sysfs_remove_group() can wait for active sysfs callbacks to drain, and those callbacks can enter the OCC update path and try to take occ->lock again. That gives the unregister paths the lock ordering occ->lock -> sysfs callback drain, while a callback has the opposite edge sysfs callback -> occ->lock. This issue was found by our static analysis tool and then manually reviewed against the current tree. The grounded PoC kept the real unregister and callback carrier: occ_shutdown() hwmon_device_unregister() occ_show_temp_1() occ_update_response() Lockdep reported the circular dependency with occ_shutdown() already holding the OCC mutex and hwmon_device_unregister() waiting on the sysfs side: WARNING: possible circular locking dependency detected ... (sysfs_lock) ... at: hwmon_device_unregister+0x12/0x30 [vuln_msv] ... (&test_occ.lock) ... at: occ_shutdown.constprop.0+0xe/0x40 [vuln_msv] occ_update_response.isra.0+0xb/0x20 [vuln_msv] occ_show_temp_1.constprop.0.isra.0+0x23/0x40 [vuln_msv] *** DEADLOCK *** Serialize hwmon registration and removal with a separate hwmon_lock. Under that lock, detach occ->hwmon and update occ->active while occ->lock is held so concurrent OCC state changes still see a stable state, then drop occ->lock before calling hwmon_device_unregister(). Remove the driver sysfs group before taking occ->lock in occ_shutdown(), so draining the driver attributes cannot wait while the OCC mutex is held. Also make OCC update callbacks return -ENODEV after deactivation, so callbacks that already passed sysfs active protection do not poll the hardware after teardown has detached the hwmon device.	N/A	More Details
CVE-2026-81675	The endpoint ‘/ws/apiprensa/getVideoUltimasSeccion’ contains an SQL injection vulnerability in the id_seccion parameter. The parameter is directly embedded in a complex SQL query that includes grouping and sorting operations. By injecting SQL syntax, an attacker can disrupt the query structure and cause database errors, exposing the internal logic of the queries. The complexity of the query increases the potential impact, as it could allow for broader manipulation of the content retrieval logic.	N/A	More Details
CVE-2026-80666	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: sco: Fix a race condition in sco_sock_timeout() sco_sock_timeout() runs asynchronously and lock_sock(sk). If the socket is closing while the timer is running, it holds the same lock (lock_sock(sk)) twice, leading to a deadlock. CPU 0 CPU 1 ==================== ==================== sco_sock_close() sco_sock_timeout() lock_sock(sk) // <-- LOCK __sco_sock_close() sco_chan_del() sco_conn_put() sco_conn_free() disable_delayed_work_sync() lock(sk) // <-- SAME LOCK Fix this by moving disable_delayed_work_sync() outside of lock_sock(sk), ensuring that no lock_sock(sk) is held before sco_sock_timeout(). Lockdep splat: WARNING: possible circular locking dependency detected 6.13.0-rc4 #7 Not tainted syz-executor292/9514 is trying to acquire lock: ffff8881115d5070 ((work_completion)(&(&conn->timeout_work)->work)){+.+.}-{0:0}, at: rcu_lock_acquire sect/v6.13-rc4/./include/linux/rcupdate.h:337 [inline] ffff8881115d5070 ((work_completion)(&(&conn->timeout_work)->work)){+.+.}-{0:0}, at: rcu_read_lock sect/v6.13-rc4/./include/linux/rcupdate.h:849 [inline] ffff8881115d5070 ((work_completion)(&(&conn->timeout_work)->work)){+.+.}-{0:0}, at: start_flush_work sect/v6.13-rc4/kernel/workqueue.c:4137 [inline] ffff8881115d5070 ((work_completion)(&(&conn->timeout_work)->work)){+.+.}-{0:0}, at: __flush_work+0xd1/0xc40 sect/v6.13-rc4/kernel/workqueue.c:4195 but task is already holding lock: ffff88807db3a258 (sk_lock-AF_BLUETOOTH-BTPROTO_SCO){+.+.}-{0:0}, at: lock_sock sect/v6.13-rc4/./include/net/sock.h:1623 [inline] ffff88807db3a258 (sk_lock-AF_BLUETOOTH-BTPROTO_SCO){+.+.}-{0:0}, at: sco_sock_close+0x25/0x100 sect/v6.13-rc4/net/bluetooth/sco.c:524 which lock already depends on the new lock. the existing dependency chain (in reverse order) is: -> #1 (sk_lock-AF_BLUETOOTH-BTPROTO_SCO){+.+.}-{0:0}: lock_acquire+0x1c4/0x520 sect/v6.13-rc4/kernel/locking/lockdep.c:5849 lock_sock_nested+0x48/0x130 sect/v6.13-rc4/net/core/sock.c:3622 lock_sock sect/v6.13-rc4/./include/net/sock.h:1623 [inline] sco_sock_timeout+0xbe/0x270 sect/v6.13-rc4/net/bluetooth/sco.c:158 process_one_work sect/v6.13-rc4/kernel/workqueue.c:3229 [inline] process_scheduled_works+0xa99/0x18f0 sect/v6.13-rc4/kernel/workqueue.c:3310 worker_thread+0x8a9/0xd80 sect/v6.13-rc4/kernel/workqueue.c:3391 kthread+0x2c6/0x360 sect/v6.13-rc4/kernel/kthread.c:389 ret_from_fork+0x4e/0x80 sect/v6.13-rc4/arch/x86/kernel/process.c:147 ret_from_fork_asm+0x1a/0x30 sect/v6.13-rc4/arch/x86/entry/entry_64.S:244 -> #0 ((work_completion)(&(&conn->timeout_work)->work)){+.+.}-{0:0}: check_prev_add sect/v6.13-rc4/kernel/locking/lockdep.c:3161 [inline] check_prevs_add sect/v6.13-rc4/kernel/locking/lockdep.c:3280 [inline] validate_chain+0x1888/0x5760 sect/v6.13-rc4/kernel/locking/lockdep.c:3904 __lock_acquire+0x13b4/0x2120 sect/v6.13-rc4/kernel/locking/lockdep.c:5226 lock_acquire+0x1c4/0x520 sect/v6.13-rc4/kernel/locking/lockdep.c:5849 touch_work_lockdep_map sect/v6.13-rc4/kernel/workqueue.c:3909 [inline] start_flush_work sect/v6.13-rc4/kernel/workqueue.c:4163 [inline] __flush_work+0x70f/0xc40 sect/v6.13-rc4/kernel/workqueue.c:4195 __cancel_work_sync sect/v6.13-rc4/kernel/workqueue.c:4351 [inline] disable_delayed_work_sync+0xbb/0xf0 sect/v6.13-rc4/kernel/workqueue.c:4514 sco_conn_free sect/v6.13-rc4/net/bluetooth/sco.c:95 [inline] kref_put sect/v6.13-rc4/./include/linux/kref.h:65 [inline] sco_conn_put+0x18f/0x270 sect/v6.13-rc4/net/bluetooth/sco.c:107 sco_chan_del+0xe2/0x210 sect/v6.13-rc4/net/bluetooth/sco.c:236	N/A	More Details

	sco_sock_close+0x8f/0x100 sect/v6.13-rc4/net/bluetooth/sco.c:526 sco_sock_release+0x62/0x2d0 sect/v6.13-rc4/net/blueto ---truncated---		
CVE-2026-80667	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: LAG, MPESW, Fix missing complete() on devcom error mlx5_mpesw_work() returned without calling complete() when mlx5_lag_get_devcom_comp() returned NULL. A caller that queued the work and waited on mpesww->comp would block indefinitely. Funnel the early-return path through a new "complete" label so the waiter is always woken.	N/A	More Details
CVE-2026-80669	In the Linux kernel, the following vulnerability has been resolved: bpf: Disable xfrm_decode_session hook attachment BPF LSM programs can currently attach to xfrm_decode_session(). That hook may return an error, but security_skb_classify_flow() calls it from a void path and triggers BUG_ON() if an error is returned. Disable BPF attachment to the hook to prevent a BPF LSM program from turning packet classification into a full panic.	N/A	More Details
CVE-2026-80676	In the Linux kernel, the following vulnerability has been resolved: Drivers: hv: vmbus: use generic driver_override infrastructure When a driver is probed through __driver_attach(), the bus' match() callback is called without the device lock held, thus accessing the driver_override field without a lock, which can cause a UAF. Fix this by using the driver-core driver_override infrastructure taking care of proper locking internally. Note that calling match() from __driver_attach() without the device lock held is intentional. [1]	N/A	More Details
CVE-2026-80679	In the Linux kernel, the following vulnerability has been resolved: s390/dasd: Fix potential NULL pointer dereference dasd_release_space() checks the implementation of the is_ese() discipline function before calling it to determine if a given device is an ESE DASD. The current usage of the logical AND operator will lead to a NULL pointer dereference as the function is called even if the function pointer is NULL. Fix this by using the logical OR operator.	N/A	More Details
CVE-2026-77991	Joomla Extension - joomlaeventmanager.net - Privileged remote code execution in Joomla Event Manager < 5.0.1 - The administrator source model allows to write dangerous file type incl. PHP, leading to remote code execution.	N/A	More Details
CVE-2026-77990	Joomla Extension - joomlaeventmanager.net - Attendee lists readable by any logged-in user in Joomla Event Manager < 5.0.1 - A non-manager can therefore read attendee names, usernames, registration dates and statuses for events they do not manage, including lists belonging to unpublished events.	N/A	More Details
CVE-2026-80686	In the Linux kernel, the following vulnerability has been resolved: mm: migrate_device: fix pte_pfn/pte_dirty called on non-present PTE pte_pfn() and pte_dirty() have undefined behaviour when called on a non-present PTE. In migrate_vma_collect_pmd(), these functions may be invoked on non-present entries (e.g., device-private entries), leading to potential crashes from pte_pfn() or incorrect dirty folio accounting from pte_dirty(). Fix both by guarding with pte_present() checks.	N/A	More Details
CVE-2026-80687	In the Linux kernel, the following vulnerability has been resolved: iommufd/viommu: Release the igroup lock on the vdevice_size error path iommufd_vdevice_alloc_ioctl() takes idev->igroup->lock, then validates the driver's vdevice_size against the core structure size with a WARN_ON_ONCE. On failure that guard jumps to out_put_idev, below out_unlock_igroup, so it skips the mutex_unlock(), leaving the igroup lock held and deadlocking the next vDEVICE operation on that group. Jump to out_unlock_igroup instead.	N/A	More Details
CVE-2026-80644	In the Linux kernel, the following vulnerability has been resolved: ocfs2: don't BUG_ON an invalid journal dinode [BUG] A fuzzed OCFS2 image can corrupt the current slot journal dinode while mount is still in progress. The mount path first reports the invalid journal block and then crashes in shutdown: kernel BUG at fs/ocfs2/journal.c:1034! Oops: invalid opcode: 0000 [#1] SMP KASAN NOPTI RIP: 0010:ocfs2_journal_toggle_dirty+0x2d6/0x340 fs/ocfs2/journal.c:1034 Call Trace: ocfs2_journal_shutdown+0x414/0xc30 fs/ocfs2/journal.c:1116 ocfs2_mount_volume fs/ocfs2/super.c:1785 [inline] ocfs2_fill_super+0x30a9/0x3cd0 fs/ocfs2/super.c:1083 get_tree_bdev_flags+0x38b/0x640 fs/super.c:1698 get_tree_bdev+0x24/0x40 fs/super.c:1721 ocfs2_get_tree+0x21/0x30 fs/ocfs2/super.c:1184 vfs_get_tree+0x9a/0x370 fs/super.c:1758 fc_mount fs/namespace.c:1199 [inline] do_new_mount_fc fs/namespace.c:3642 [inline] do_new_mount fs/namespace.c:3718 [inline] path_mount+0x5b8/0x1ea0 fs/namespace.c:4028 do_mount fs/namespace.c:4041 [inline] __do_sys_mount fs/namespace.c:4229 [inline] __se_sys_mount fs/namespace.c:4206 [inline] __x64_sys_mount+0x282/0x320 fs/namespace.c:4206 ... [CAUSE] ocfs2_journal_toggle_dirty() used to return -EIO when journal->j_bh no longer contained a valid dinode, because the startup and shutdown paths already handled that failure. Commit 10995aa2451a ("ocfs2: Morph the haphazard OCFS2_IS_VALID_DINODE() checks.") changed the check to a BUG_ON() under the assumption that the journal dinode had already been validated. That turns an unexpected invalid journal dinode during mount teardown into a kernel crash instead of a normal mount failure. [FIX] Replace the BUG_ON() with WARN_ON() and return -EIO. This keeps the invariant warning for debugging, but restores the original behavior of failing startup or shutdown cleanly instead of panicking the kernel.	N/A	More Details
CVE-2026-80643	In the Linux kernel, the following vulnerability has been resolved: EDAC/igen6: Fix call trace due to missing release() When unloading the igen6_edac driver, there is a call trace: Device '(null)' does not have a release() function, it is broken and must be fixed. See Documentation/core-api/kobject.rst. WARNING: drivers/base/core.c:2567 at device_release+0x84/0x90, CPU#5: rmmod/127209 ... RIP: 0010:device_release+0x84/0x90 Call Trace: <TASK> kobject_put+0x8c/0x220 put_device+0x17/0x30 igen6_unregister_mcis+0xa2/0xe0 [igen6_edac] igen6_remove+0x82/0xb0 [igen6_edac] ... Fix the call trace by providing empty release() functions for the memory controller devices.	N/A	More Details

CVE-2026-80642	In the Linux kernel, the following vulnerability has been resolved: liveupdate: Reference count incoming FLB data Increment the incoming FLB refcount in liveupdate_flb_get_incoming() so that the FLB structure cannot be freed while the caller is actively using it. Add an additional liveupdate_flb_put_incoming() function so the caller can explicitly indicate when it is done using the FLB data. During a Live Update, a subsystem might need to hold onto the incoming File-Lifecycle-Bound (FLB) data for an extended period, such as during device enumeration. Incrementing the reference count guarantees that the data remains valid and accessible until the subsystem releases it, preventing future use-after-free bugs.	N/A	More Details
CVE-2026-80641	In the Linux kernel, the following vulnerability has been resolved: wifi: wlcore: enable the right set of ciphers The firmware version number check for IGTK introduced in commit c34dbc5900b0 ("wifi: wlcore: Add support for IGTK key") lets the amount of ciphers decrease on every boot of a too old firmware and that is practically happening. It also does not take into account other chips than the wl18xx. On some wl128x, the following can be observed when connecting via nm to a common ap: [484.113311] wlcore: WARNING could not set keys [484.117828] wlcore: ERROR Could not add or replace key [484.123016] wlan0: failed to set key (5, ff:ff:ff:ff:ff:ff) to hardware (-5) [484.123046] wlcore: Hardware recovery in progress. FW ver: Rev 7.3.10.0.142 [484.139923] wlcore: pc: 0x0, hint_sts: 0x00000048 count: 1 [484.145721] wlcore: down [484.148986] ieee80211 phy0: Hardware restart was requested [484.610473] wlcore: firmware booted (Rev 7.3.10.0.142) [484.633758] wlcore: Association completed. [484.690490] wlcore: ERROR command execute failure 14 [484.690490] ------------[cut here]------------ [484.700195] WARNING: drivers/net/wireless/ti/wlcore/main.c:872 at wl12xx_queue_recovery_work+0x64/0x74 [wlcore], CPU#0: kworker/0:0/892 This repeats endlessly. Always disable IGTK on wl12xx and fix the decrementing mess.	N/A	More Details
CVE-2026-81674	The endpoint ‘/ws/apiprensa/getVideoNextPrev’ is vulnerable to SQL injection via the id_ambito parameter. Unsanitized input is directly incorporated into a MariaDB query, allowing attackers to inject SQL syntax that interrupts the query's execution. The vulnerability results in detailed database error messages and exposes the internal structure of the queries, which could facilitate further exploitation.	N/A	More Details
CVE-2026-81673	The ‘/ws/apitribuna/setVisita’ endpoint is vulnerable to SQL injection through the id_video and id_ambito parameters. The application does not validate or sanitize these inputs before including them in SQL queries. This allows a remote attacker to inject SQL syntax and disrupt the execution of queries, causing database errors and potentially manipulating visit tracking records. Given the nature of the endpoint, this could also affect the integrity of analytics and the accuracy of records.	N/A	More Details
CVE-2026-80616	In the Linux kernel, the following vulnerability has been resolved: ieee802154: Avoid calling WARN_ON() on -ENOMEM in cfg802154_switch_netns() It's pointless to call WARN_ON() in case of an allocation failure in dev_change_net_namespace() and device_rename(), since it only leads to useless splats caused by deliberate fault injections, so avoid it. Found by Linux Verification Center (linuxtesting.org) with Syzkaller.	N/A	More Details
CVE-2026-80618	In the Linux kernel, the following vulnerability has been resolved: drm/amdkfd: Avoid double-unpin of DOORBELL/MMIO BOs on free amdgpu_amdkfd_gpuvm_free_memory_of_gpu() unpinned DOORBELL and MMIO remap BOs (which are pinned at allocation time) before checking whether the BO is still mapped to the GPU. When the BO is still mapped, the function returns -EBUSY and leaves the BO alive, but it has already been unpinned. The BO is then unpinned again when it is finally freed during process teardown, triggering a ttm_bo_unpin() underflow warning: WARNING: CPU: 18 PID: 15066 at ttm/ttm_bo.c:650 amdttm_bo_unpin+0x6d/0x80 [amdttm] Workqueue: kfd_process_wq kfd_process_wq_release [amdgpu] RIP: 0010:amdttm_bo_unpin+0x6d/0x80 [amdttm] Call Trace: amdgpu_bo_unpin+0x1a/0x90 [amdgpu] amdgpu_amdkfd_gpuvm_unpin_bo+0x31/0xb0 [amdgpu] amdgpu_amdkfd_gpuvm_free_memory_of_gpu+0x3bf/0x460 [amdgpu] kfd_process_free_outstanding_kfd_bos+0xd4/0x170 [amdgpu] kfd_process_wq_release+0x109/0x1b0 [amdgpu] process_one_work+0x1e2/0x3b0 worker_thread+0x50/0x3a0 kthread+0xdd/0x100 ret_from_fork+0x29/0x50 Move the unpin after the mapped_to_gpu_memory check so it only happens once we are committed to freeing the BO. (cherry picked from commit 927c5b2defb9b09856444d94bebfd056a002bd75)	N/A	More Details
CVE-2026-81672	SQL injection vulnerability in the ‘/ws/apiprensa/getVideoSubcanal’ endpoint due to improper handling of the id_video parameter. The application does not sanitize input before constructing SQL queries, which results in execution errors when malicious input is provided. The vulnerability exposes internal file paths and complete stack traces through the Slim framework’s error handler, which increases the severity due to the combination of information disclosure and SQL injection.	N/A	More Details
CVE-2026-80620	In the Linux kernel, the following vulnerability has been resolved: Revert "PCI/MSI: Unmap MSI-X region on error" This reverts commit 1a8d4c6ecb4c81261bcdf13556abd4a958eca202. Commit 1a8d4c6ecb4c ("PCI/MSI: Unmap MSI-X region on error") added an iounmap(dev->msix_base) on the error path of msix_capability_init() to release the MSI-X region when msix_setup_interrupts() fails. When msix_setup_interrupts() fails, the call chain is: msix_setup_interrupts() -> __msix_setup_interrupts() struct pci_dev *dev __free(free_msi_irqs) = __dev; ... return ret; // __free cleanup fires on error The __free(free_msi_irqs) cleanup calls pci_free_msi_irqs(), which already handles the unmap: void pci_free_msi_irqs(struct pci_dev *dev) { pci_msi_teardown_msi_irqs(dev); if (dev->msix_base) { iounmap(dev->msix_base); // already unmapped here dev->msix_base = NULL; // and set to NULL } } So dev->msix_base is unmapped and set to NULL before msix_setup_interrupts() returns to msix_capability_init(). The "goto out_unmap" introduced by commit 1a8d4c6ecb4c ("PCI/MSI: Unmap MSI-X region on error") then calls iounmap() a second time on a NULL pointer. This was reproduced on Intel	N/A	More Details

	Emerald Rapids (192 CPUs) while running tools/testing/selftests/kexec/test_kexec_jump.sh: WARNING: CPU#44 at iounmap+0x2a/0xe0 RIP: 0010:iounmap+0x2a/0xe0 RDI: 0000000000000000 Call Trace: msix_capability_init+0x317/0x3f0 __pci_enable_msix_range+0x21d/0x2c0 pci_alloc_irq_vectors_affinity+0xa9/0x130 nvme_setup_io_queues+0x2a8/0x420 [nvme] nvme_reset_work+0x151/0x340 [nvme] ... RDI=0 confirms iounmap() is called with NULL. Restore the original "goto out_disable" and leave the unmap to the existing __free(free_msi_irqs) cleanup.		
CVE-2026-80621	In the Linux kernel, the following vulnerability has been resolved: PCI: dwc: Avoid dwc_pcie_rasdes_debugfs_deinit() NULL dereference when no RAS DES capability dwc_pcie_rasdes_debugfs_init() returns success when the controller has no RAS DES capability, leaving pci->debugfs->rasdes_info unset. The common debugfs teardown path still calls dwc_pcie_rasdes_debugfs_deinit(), which dereferences rasdes_info unconditionally. Return early when no RAS DES state was allocated. In that case no RAS DES mutex was initialized, so there is nothing to destroy. [mani: reworded subject]	N/A	More Details
CVE-2026-80623	In the Linux kernel, the following vulnerability has been resolved: coresight: ete: Always save state on power down System register ETMs and ETE are unlikely to be preserved on CPU power down. The ETE DT binding also never documented "arm,coresight-loses-context-with-cpu" so nobody would have legitimately been able to use that binding to fix it and ACPI has no such binding at all. Fix it by hard coding the setting for sysreg ETMs (ETE is always sysreg) or ACPI boots. Use a local variable when setting up save_state so that it's immune to concurrent probing when devices have different configurations which is an issue with modifying the global. This fixes the following error when using Coresight with ACPI on the FVP which supports CPU PM: coresight ete0: External agent took claim tag WARNING: drivers/hwtracing/coresight/coresight-core.c:248 at coresight_disclaim_device_unlocked+0xe0/0xe8, CPU#0: perf/117	N/A	More Details
CVE-2026-80624	In the Linux kernel, the following vulnerability has been resolved: mfd: cs42l43: Sanity check firmware size Currently the code checks if a firmware was received, however it does not verify that the firmware size is larger than the firmware header. As the firmware pointer is dereferenced as a pointer to the header structure this could lead to an out of bounds memory access. Add the missing check.	N/A	More Details
CVE-2026-80625	In the Linux kernel, the following vulnerability has been resolved: RDMA/hns: Fix memory leak of bonding resources In a corner case of concurrent driver removal and driver reset, bonding resource is first released in hns_roce_hw_v2_exit() during driver removal, and then is allocated again in hns_roce_register_device() during driver reset. This leads to memory leak because the release timing has already passed. This may also lead to a kernel panic as below because of the leaked notifier callback: Call trace: 0xffffa20fccc04978 (P) raw_notifier_call_chain+0x20/0x38 call_netdevice_notifiers_info+0x60/0xb8 netdev_lower_state_changed+0x4c/0xb8 As Sashiko suggested, the teardown order of bonding resources should be inverted to make sure the resources are released when the driver is removed.	N/A	More Details
CVE-2026-80626	In the Linux kernel, the following vulnerability has been resolved: powerpc/perf: fix preempt count underflow in fsl_emb_pmu_del fsl_emb_pmu_del() unconditionally calls put_cpu_var(cpu_hw_events) at the 'out:' label, but only calls the matching get_cpu_var() after the 'i < 0' early-return check. When event->hw.idx is negative the function jumps to 'out:' without having taken get_cpu_var(), and the trailing put_cpu_var() then issues an unmatched preempt_enable(), underflowing preempt_count. On a CONFIG_PREEMPT=y kernel preempt_count would underflow and eventually present as a 'scheduling while atomic' BUG. Move put_cpu_var() to pair with get_cpu_var() so the percpu access is correctly bracketed and the 'out:' label only handles perf_pmu_enable.	N/A	More Details
CVE-2026-80627	In the Linux kernel, the following vulnerability has been resolved: MIPS: mm: Fix out-of-bounds write in maar_res_walk() maar_res_walk() uses wi->num_cfg as the index into the fixed-size wi->cfg array, but checks whether the array is full only after it has filled the selected entry. If walk_system_ram_range() reports more than 16 memory ranges, the overflow call writes one struct maar_config past the end of the array before WARN_ON() prevents num_cfg from advancing. Move the full-array check before taking the array slot and return non-zero when the scratch array is full, so walk_system_ram_range() terminates the walk instead of invoking the callback for further ranges.	N/A	More Details
CVE-2026-81662	Affected versions of Flowintel improperly trust configuration keys supplied to the alerts settings update endpoint. While configuration values were normalized to Python literals, the corresponding keys were used directly when constructing and replacing lines in conf/config_module.py. The vulnerable code used requester-controlled keys in both the regular expression and the generated assignment: f'{key} = {py_val}' and appended an assignment if the key was not already present. The modified Python configuration module was subsequently reloaded using importlib.reload(). This creates a code-generation boundary in which specially crafted configuration keys can alter the Python source structure and result in execution of attacker-controlled Python statements. Version impacted >=3.3.0	N/A	More Details
CVE-2026-80629	In the Linux kernel, the following vulnerability has been resolved: octeontx2-af: npc: Fix size of entry2cntr_map KASAN prints below splat. This is caused by allocating counter for reserved mcam entry for cpt 2nd pass entry. But mcam->entry2cntr_map is not allocated for reserved entries. BUG: KASAN: slab-out-of-bounds in npc_map_mcam_entry_and_cntr+0xb0/0x1a0 Write of size 2 at addr ffff0001033e7ffe by task kworker/0:1/14 CPU: 0 PID: 14 Comm: kworker/0:1 Not tainted 6.1.67 #1 Hardware name: Marvell CN106XX board (DT) Workqueue: events work_for_cpu_fn Call trace: dump_backtrace.part.0+0xe4/0xf0 show_stack+0x18/0x30 dump_stack_lvl+0x88/0xb4 print_report+0x154/0x458 kasan_report+0xb8/0x194 __asan_store2+0x7c/0xa0 npc_map_mcam_entry_and_cntr+0xb0/0x1a0	N/A	More Details

	rvu_mbox_handler_npc_mcam_write_entry+0x268/0x280 npc_install_flow+0x840/0xfe0 rvu_npc_install_cpt_pass2_entry+0x138/0x190 rvu_nix_init+0x148c/0x2880 rvu_probe+0x1800/0x30b0 local_pci_probe+0x78/0xe0 work_for_cpu_fn+0x30/0x50 process_one_work+0x4cc/0x97c worker_thread+0x360/0x630 kthread+0x1a0/0x1b0 ret_from_fork+0x10/0x20		
CVE-2026-81659	Affected versions of Flowintel allow attacker-controlled note content to be processed by Pandoc and XeLaTeX during PDF export in a way that can cause local files on the Flowintel server to be read and incorporated into the generated export.	N/A	More Details
CVE-2026-80632	In the Linux kernel, the following vulnerability has been resolved: wifi: mt76: mt7996: Fix NULL pointer dereference in mt7996_init_tx_queues() When MT76_NPU and CONFIG_NET_MEDIATEK_SOC_WED are enabled and mt76 detects properly the Airoha NPU SoC, mt7996_init_tx_queues() will dereference a NULL WED pointer. Fix the issue by always passing the WED pointer from mt7996_dma_init().	N/A	More Details
CVE-2026-80636	In the Linux kernel, the following vulnerability has been resolved: netfilter: conntrack: revert ct extension genid infrastructure This infrastructure is not used anymore after moving ct timeout and helper to use datapath refcount to track object use. Revert commit c56716c69ce1 ("netfilter: extensions: introduce extension genid count") this patch disables all ct extensions (leading to NULL) for unconfirmed conntracks, when this is only targeted at ct helper and ct timeout. There is also codebase that dereferences the ct extension without checking for NULL which could lead to crash.	N/A	More Details
CVE-2026-80639	In the Linux kernel, the following vulnerability has been resolved: cxl/test: Fix __fortify_panic Fix a runtime assertion in setup_xor_mapping(). Fortify complains that it is potentially overflowing the xormaps array per __counted_by(nr_maps). Quiet the false positive by initializing @nr_maps earlier. memcpy: detected buffer overflow: 32 byte write of buffer size 0 WARNING: lib/string_helpers.c:1036 at __fortify_report+0x4d/0xa0, CPU#8: modprobe/2728 Call Trace: __fortify_panic+0xd/0xf setup_xor_mapping+0x6c/0xa0 [cxl_translate] [dj: Fixed up @nr_entries to @nr_maps in commit log.]	N/A	More Details
CVE-2026-80640	In the Linux kernel, the following vulnerability has been resolved: cxl/fwctl: Fix __fortify_panic Fix a runtime assertion in cxlctl_get_supported_features(). Fortify complains that it is potentially overflowing the entries array per __counted_by_le(num_entries). Quiet the false positive by initializing @num_entries earlier. memcpy: detected buffer overflow: 48 byte write of buffer size 0 WARNING: lib/string_helpers.c:1036 at __fortify_report+0x4d/0xa0, CPU#7: fwctl/1398 RIP: 0010:__fortify_report+0x50/0xa0 Call Trace: __fortify_panic+0xd/0xf cxlctl_get_supported_features.cold+0x23/0x35 [cxl_core]	N/A	More Details
CVE-2026-19314	An integer underflow vulnerability in the WatchGuard Fireware OS iked process allows a remote unauthenticated attacker to create a Denial of Service (DoS) condition in VPN processing by sending specially crafted network traffic.	N/A	More Details