SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 11 February 2026

Generated on 11 February 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-2026-1633	The Synectix LAN 232 TRIO 3-Port serial to ethernet adapter exposes its web management interface without requiring authentication, allowing unauthenticated users to modify critical device settings or factory reset the device.	10.0	More Details
CVE-2025-68121	During session resumption in crypto/tls, if the underlying Config has its ClientCAs or RootCAs fields mutated between the initial handshake and the resumed handshake, the resumed handshake may succeed when it should have failed. This may happen when a user calls Config.Clone and mutates the returned Config, or uses Config.GetConfigForClient. This can cause a client to resume a session with a server that it would not have resumed with during the initial handshake, or cause a server to resume a session with a client that it would not have resumed with during the initial handshake.	10.0	More Details
CVE-2026-25632	EPyT-Flow is a Python package designed for the easy generation of hydraulic and water quality scenario data of water distribution networks. Prior to 0.16.1, EPyT-Flow's REST API parses attacker-controlled JSON request bodies using a custom deserializer (my_load_from_json) that supports a type field. When type is present, the deserializer dynamically imports an attacker-specified module/class and instantiates it with attacker-supplied arguments. This allows invoking dangerous classes such as subprocess.Popen, which can lead to OS command execution during JSON parsing. This also affects the loading of JSON files. This vulnerability is fixed in 0.16.1.	10.0	More Details
CVE-2026-25641	SandboxJS is a JavaScript sandboxing library. Prior to 0.8.29, there is a sandbox escape vulnerability due to a mismatch between the key on which the validation is performed and the key used for accessing properties. Even though the key used in property accesses is annotated as string, this is never enforced. So, attackers can pass malicious objects that coerce to different string values when used, e.g., one for the time the key is sanitized using hasOwnProperty(key) and a different one for when the key is used for the actual	10.0	More Details

	property access. This vulnerability is fixed in 0.8.29.		
CVE-2026-25587	SandboxJS is a JavaScript sandboxing library. Prior to 0.8.29, as Map is in SAFE_PROTOYPES, it's prototype can be obtained via Map.prototype. By overwriting Map.prototype.has the sandbox can be escaped. This vulnerability is fixed in 0.8.29.	10.0	More Details
CVE-2025-59818	This vulnerability allows authenticated attackers to execute arbitrary commands on the underlying system using the file name of an uploaded file.	10.0	More Details
CVE-2026-25520	SandboxJS is a JavaScript sandboxing library. Prior to 0.8.29, The return values of functions aren't wrapped. Object.values/Object.entries can be used to get an Array containing the host's Function constructor, by using Array.prototype.at you can obtain the hosts Function constructor, which can be used to execute arbitrary code outside of the sandbox. This vulnerability is fixed in 0.8.29.	10.0	More Details
CVE-2026-25725	Claude Code is an agentic coding tool. Prior to version 2.1.2, Claude Code's bubblewrap sandboxing mechanism failed to properly protect the .claude/settings.json configuration file when it did not exist at startup. While the parent directory was mounted as writable and .claude/settings.local.json was explicitly protected with read-only constraints, settings.json was not protected if it was missing. This allowed malicious code running inside the sandbox to create this file and inject persistent hooks (such as SessionStart commands) that would execute with host privileges when Claude Code was restarted. This issue has been patched in version 2.1.2.	10.0	More Details
CVE-2026-25586	SandboxJS is a JavaScript sandboxing library. Prior to 0.8.29, a sandbox escape is possible by shadowing hasOwnProperty on a sandbox object, which disables prototype whitelist enforcement in the property-access path. This permits direct access to __proto__ and other blocked prototype properties, enabling host Object.prototype pollution and persistent cross-sandbox impact. This vulnerability is fixed in 0.8.29.	10.0	More Details
CVE-2026-26009	Catalyst is a platform built for enterprise game server hosts, game communities, and billing panel integrations. Install scripts defined in server templates execute directly on the host operating system as root via bash -c, with no sandboxing or containerization. Any user with template.create or template.update permission can define arbitrary shell commands that achieve full root-level remote code execution on every node machine in the cluster. This vulnerability is fixed in commit 11980aaf3f46315b02777f325ba02c56b110165d.	9.9	More Details
CVE-2026-0488	An authenticated attacker in SAP CRM and SAP S/4HANA (Scripting Editor) could exploit a flaw in a generic function module call and execute unauthorized critical functionalities, which includes the ability to execute an arbitrary SQL statement. This leads to a full database compromise with high impact on confidentiality, integrity, and availability.	9.9	More Details
CVE-2026-25052	n8n is an open source workflow automation platform. Prior to versions 1.123.18 and 2.5.0, a vulnerability in the file access controls allows authenticated users with permission to create or modify workflows to read sensitive files from the n8n host system. This can be exploited to obtain critical configuration data and user credentials, leading to complete account takeover of any user on the instance. This issue has been patched in versions 1.123.18 and 2.5.0.	9.9	More Details
CVE-2026-25053	n8n is an open source workflow automation platform. Prior to versions 1.123.10 and 2.5.0, vulnerabilities in the Git node allowed authenticated users with permission to create or modify workflows to execute arbitrary system commands or read arbitrary files on the n8n host. This issue has been patched in versions 1.123.10 and 2.5.0.	9.9	More Details
CVE-2026-25115	n8n is an open source workflow automation platform. Prior to version 2.4.8, a vulnerability in the Python Code node allows authenticated users to break out of the Python sandbox environment and execute code outside the intended security boundary. This issue has been patched in version 2.4.8.	9.9	More Details
CVE-	Semantic Kernel is an SDK used to build, orchestrate, and deploy AI agents and multi-agent systems. Prior to 1.70.0, an Arbitrary File Write vulnerability has been identified in Microsoft's Semantic Kernel .NET SDK, specifically within the SessionsPythonPlugin. The		More

2026-25592	problem has been fixed in Microsoft.SemanticKernel.Core version 1.70.0. As a mitigation, users can create a Function Invocation Filter which checks the arguments being passed to any calls to DownloadFileAsync or UploadFileAsync and ensures the provided localFilePath is allow listed.	9.9	Details
CVE-2026-1868	GitLab has remediated a vulnerability in the Duo Workflow Service component of GitLab AI Gateway affecting all versions of the AI Gateway from 18.1.6, 18.2.6, 18.3.1 to 18.6.1, 18.7.0, and 18.8.0 in which AI Gateway was vulnerable to insecure template expansion of user supplied data via crafted Duo Agent Platform Flow definitions. This vulnerability could be used to cause Denial of Service or gain code execution on the Gateway. This has been fixed in versions 18.6.2, 18.7.1, and 18.8.1 of the GitLab AI Gateway.	9.9	More Details
CVE-2026-25049	n8n is an open source workflow automation platform. Prior to versions 1.123.17 and 2.5.2, an authenticated user with permission to create or modify workflows could abuse crafted expressions in workflow parameters to trigger unintended system command execution on the host running n8n. This issue has been patched in versions 1.123.17 and 2.5.2.	9.9	More Details
CVE-2025-6830	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Xpoda Türkiye Information Technology Inc. Xpoda Studio allows SQL Injection.This issue affects Xpoda Studio: through 09022026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	9.8	More Details
CVE-2020-37159	Parallaxis Cuckoo Clock 5.0 contains a buffer overflow vulnerability that allows attackers to execute arbitrary code by overwriting memory registers in the alarm scheduling feature. Attackers can craft a malicious payload exceeding 260 bytes to overwrite EIP and EBP, enabling shellcode execution with potential remote code execution.	9.8	More Details
CVE-2026-21531	Deserialization of untrusted data in Azure SDK allows an unauthorized attacker to execute code over a network.	9.8	More Details
CVE-2026-23906	Affected Products and Versions * Apache Druid * Affected Versions: 0.17.0 through 35.x (all versions prior to 36.0.0) * Prerequisites: * druid-basic-security extension enabled * LDAP authenticator configured * Underlying LDAP server permits anonymous bind Vulnerability Description An authentication bypass vulnerability exists in Apache Druid when using the druid-basic-security extension with LDAP authentication. If the underlying LDAP server is configured to allow anonymous binds, an attacker can bypass authentication by providing an existing username with an empty password. This allows unauthorized access to otherwise restricted Druid resources without valid credentials. The vulnerability stems from improper validation of LDAP authentication responses when anonymous binds are permitted, effectively treating anonymous bind success as valid user authentication. Impact A remote, unauthenticated attacker can: * Gain unauthorized access to the Apache Druid cluster * Access sensitive data stored in Druid datasources * Execute queries and potentially manipulate data * Access administrative interfaces if the bypassed account has elevated privileges * Completely compromise the confidentiality, integrity, and availability of the Druid deployment Mitigation Immediate Mitigation (No Druid Upgrade Required): * Disable anonymous bind on your LDAP server. This prevents the vulnerability from being exploitable and is the recommended immediate action. Resolution * Upgrade Apache Druid to version 36.0.0 or later, which includes fixes to properly reject anonymous LDAP bind attempts.	9.8	More Details
CVE-2025-11242	Server-Side Request Forgery (SSRF) vulnerability in Teknolist Computer Systems Software Publishing Industry and Trade Inc. Okulistik allows Server Side Request Forgery.This issue affects Okulistik: through 21102025.	9.8	More Details
CVE-2025-13375	IBM Common Cryptographic Architecture (CCA) 7.5.52 and 8.4.82 could allow an unauthenticated user to execute arbitrary commands with elevated privileges on the system.	9.8	More Details
	Payload is a free and open source headless content management system. Prior to 3.73.0,		

CVE-2026-25544	when querying JSON or richText fields, user input was directly embedded into SQL without escaping, enabling blind SQL injection attacks. An unauthenticated attacker could extract sensitive data (emails, password reset tokens) and achieve full account takeover without password cracking. This vulnerability is fixed in 3.73.0.	9.8	More Details
CVE-2026-25803	3DP-MANAGER is an inbound generator for 3x-ui. In version 2.0.1 and prior, the application automatically creates an administrative account with known default credentials (admin/admin) upon the first initialization. Attackers with network access to the application's login interface can gain full administrative control, managing VPN tunnels and system settings. This issue will be patched in version 2.0.2.	9.8	More Details
CVE-2020-37095	Cyberoam Authentication Client 2.1.2.7 contains a buffer overflow vulnerability that allows remote attackers to execute arbitrary code by overwriting Structured Exception Handler (SEH) memory. Attackers can craft a malicious input in the 'Cyberoam Server Address' field to trigger a bind TCP shell on port 1337 with system-level access.	9.8	More Details
CVE-2020-37161	Wedding Slideshow Studio 1.36 contains a buffer overflow vulnerability that allows attackers to execute arbitrary code by overwriting the registration name field with malicious payload. Attackers can craft a specially designed payload to trigger remote code execution, demonstrating the ability to run system commands like launching the calculator.	9.8	More Details
CVE-2026-22906	User credentials are stored using AES-ECB encryption with a hardcoded key. An unauthenticated remote attacker obtaining the configuration file can decrypt and recover plaintext usernames and passwords, especially when combined with the authentication bypass.	9.8	More Details
CVE-2020-37162	Wedding Slideshow Studio 1.36 contains a buffer overflow vulnerability in the registration key input that allows attackers to execute arbitrary code by overwriting memory. Attackers can craft a malicious payload of 1608 bytes to trigger a stack-based buffer overflow and execute commands through the registration key field.	9.8	More Details
CVE-2026-25560	WeKan versions prior to 8.19 contain an LDAP filter injection vulnerability in LDAP authentication. User-supplied username input is incorporated into LDAP search filters and DN-related values without adequate escaping, allowing an attacker to manipulate LDAP queries during authentication.	9.8	More Details
CVE-2025-15027	The JAY Login & Register plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 2.6.03. This is due to the plugin allowing a user to update arbitrary user meta through the 'jay_login_register_ajax_create_final_user' function. This makes it possible for unauthenticated attackers to elevate their privileges to that of an administrator.	9.8	More Details
CVE-2026-2096	Agentflow developed by Flowring has a Missing Authentication vulnerability, allowing unauthenticated remote attackers to read, modify, and delete database contents by using a specific functionality.	9.8	More Details
CVE-2026-2095	Agentflow developed by Flowring has an Authentication Bypass vulnerability, allowing unauthenticated remote attackers to exploit a specific functionality to obtain arbitrary user authentication token and log into the system as any user.	9.8	More Details
CVE-2026-22903	An unauthenticated remote attacker can send a crafted HTTP request containing an overly long SESSIONID cookie. This can trigger a stack buffer overflow in the modified lighttpd server, causing it to crash and potentially enabling remote code execution due to missing stack protections.	9.8	More Details
CVE-2026-22904	Improper length handling when parsing multiple cookie fields (including TRACKID) allows an unauthenticated remote attacker to send oversized cookie values and trigger a stack buffer overflow, resulting in a denial-of-service condition and possible remote code execution.	9.8	More Details
CVE-	All versions of the package jsonpath are vulnerable to Arbitrary Code Injection via unsafe evaluation of user-supplied JSON Path expressions. The library relies on the static-eval module to process JSON Path input, which is not designed to handle untrusted data safely.		

2026-1615	An attacker can exploit this vulnerability by supplying a malicious JSON Path expression that, when evaluated, executes arbitrary JavaScript code, leading to Remote Code Execution in Node.js environments or Cross-site Scripting (XSS) in browser contexts. This affects all methods that evaluate JSON Paths against objects, including .query, .nodes, .paths, .value, .parent, and .apply.	9.8	More Details
CVE-2026-25505	Bambuddy is a self-hosted print archive and management system for Bambu Lab 3D printers. Prior to version 0.1.7, a hardcoded secret key used for signing JWTs is checked into source code and ManyAPI routes do not check authentication. This issue has been patched in version 0.1.7.	9.8	More Details
CVE-2025-5329	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Martcode Software Inc. Delta Course Automation allows SQL Injection.This issue affects Delta Course Automation: through 04022026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	9.8	More Details
CVE-2026-24300	Azure Front Door Elevation of Privilege Vulnerability	9.8	More Details
CVE-2020-37125	Edimax EW-7438RPn-v3 Mini 1.27 contains a remote code execution vulnerability that allows unauthenticated attackers to execute arbitrary commands through the /goform/mp endpoint. Attackers can exploit the vulnerability by sending crafted POST requests with command injection payloads to download and execute malicious scripts on the device.	9.8	More Details
CVE-2020-37123	Pinger 1.0 contains a remote code execution vulnerability that allows attackers to inject shell commands through the ping and socket parameters. Attackers can exploit the unsanitized input in ping.php to write arbitrary PHP files and execute system commands by appending shell metacharacters.	9.8	More Details
CVE-2020-37126	Free Desktop Clock 3.0 contains a stack overflow vulnerability in the Time Zones display name input that allows attackers to overwrite Structured Exception Handler (SEH) registers. Attackers can exploit the vulnerability by crafting a malicious Unicode input that triggers an access violation and potentially execute arbitrary code.	9.8	More Details
CVE-2020-37129	Memu Play 7.1.3 contains an insecure folder permissions vulnerability that allows low-privileged users to modify the MemuService.exe executable. Attackers can replace the service executable with a malicious file during system restart to gain SYSTEM-level privileges by exploiting unrestricted file modification permissions.	9.8	More Details
CVE-2020-37138	10-Strike Network Inventory Explorer 9.03 contains a buffer overflow vulnerability in the file import functionality that allows remote attackers to execute arbitrary code. Attackers can craft a malicious text file with carefully constructed payload to trigger a stack-based buffer overflow and bypass data execution prevention through a ROP chain.	9.8	More Details
CVE-2020-37120	Rubo DICOM Viewer 2.0 contains a buffer overflow vulnerability in the DICOM server name input field that allows attackers to overwrite Structured Exception Handler (SEH). Attackers can craft a malicious text file with carefully constructed payload to execute arbitrary code by overwriting SEH and triggering remote code execution.	9.8	More Details
CVE-2020-37119	Nsauditor 3.0.28 and 3.2.1.0 contains a buffer overflow vulnerability in the DNS Lookup tool that allows attackers to execute arbitrary code by overwriting memory. Attackers can craft a malicious DNS query payload to trigger a three-byte overwrite, bypass ASLR, and execute shellcode through a carefully constructed exploit.	9.8	More Details
CVE-2026-1499	The WP Duplicate plugin for WordPress is vulnerable to Missing Authorization leading to Arbitrary File Upload in all versions up to and including 1.1.8. This is due to a missing capability check on the `process_add_site()` AJAX action combined with path traversal in the file upload functionality. This makes it possible for authenticated (subscriber-level) attackers to set the internal `prod_key_random_id` option, which can then be used by an unauthenticated attacker to bypass authentication checks and write arbitrary files to the server via the `handle_upload_single_big_file()` function, ultimately leading to remote code execution.	9.8	More Details

CVE-2026-21643	An improper neutralization of special elements used in an sql command ('sql injection') vulnerability in Fortinet FortiClientEMS 7.4.4 may allow an unauthenticated attacker to execute unauthorized code or commands via specifically crafted HTTP requests.	9.8	More Details
CVE-2026-2017	A vulnerability was detected in IP-COM W30AP up to 1.0.0.11(1340). Affected by this issue is the function R7WebsSecurityHandler of the file /goform/wx3auth of the component POST Request Handler. The manipulation of the argument data results in stack-based buffer overflow. The attack may be performed from remote. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	9.8	More Details
CVE-2025-64712	The unstructured library provides open-source components for ingesting and pre-processing images and text documents, such as PDFs, HTML, Word docs, and many more. Prior to version 0.18.18, a path traversal vulnerability in the partition_msg function allows an attacker to write or overwrite arbitrary files on the filesystem when processing malicious MSG files with attachments. This issue has been patched in version 0.18.18.	9.8	More Details
CVE-2026-25526	JinJava is a Java-based template engine based on django template syntax, adapted to render jinja templates. Prior to versions 2.7.6 and 2.8.3, JinJava is vulnerable to arbitrary Java execution via bypass through ForTag. This allows arbitrary Java class instantiation and file access bypassing built-in sandbox restrictions. This issue has been patched in versions 2.7.6 and 2.8.3.	9.8	More Details
CVE-2020-37124	B64dec 1.1.2 contains a buffer overflow vulnerability that allows attackers to execute arbitrary code by overwriting Structured Exception Handler (SEH) with crafted input. Attackers can leverage an egg hunter technique and carefully constructed payload to inject and execute malicious code during base64 decoding process.	9.8	More Details
CVE-2026-0509	SAP NetWeaver Application Server ABAP and ABAP Platform allows an authenticated, low-privileged user to perform background Remote Function Calls without the required S_RFC authorization in certain cases. This can result in a high impact on integrity and availability, and no impact on the confidentiality of the application.	9.6	More Details
CVE-2026-1709	A flaw was found in Keylime. The Keylime registrar, since version 7.12.0, does not enforce client-side Transport Layer Security (TLS) authentication. This authentication bypass vulnerability allows unauthenticated clients with network access to perform administrative operations, including listing agents, retrieving public Trusted Platform Module (TPM) data, and deleting agents, by connecting without presenting a client certificate.	9.4	More Details
CVE-2026-0106	In vpu_mmap of vpu_ioctl, there is a possible arbitrary address mmap due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	9.3	More Details
CVE-2026-25057	MarkUs is a web application for the submission and grading of student assignments. Prior to 2.9.1, instructors are able to upload a zip file to create an assignment from an exported configuration (courses/<:course_id>/assignments/upload_config_files). The uploaded zip file entry names are used to create paths to write files to disk without checking these paths. This vulnerability is fixed in 2.9.1.	9.1	More Details
CVE-2026-25539	SiYuan is a personal knowledge management system. Prior to version 3.5.5, the /api/file/copyFile endpoint does not validate the dest parameter, allowing authenticated users to write files to arbitrary locations on the filesystem. This can lead to Remote Code Execution (RCE) by writing to sensitive locations such as cron jobs, SSH authorized_keys, or shell configuration files. This issue has been patched in version 3.5.5.	9.1	More Details
CVE-2026-25643	Frigate is a network video recorder (NVR) with realtime local object detection for IP cameras. Prior to 0.16.4, a critical Remote Command Execution (RCE) vulnerability has been identified in the Frigate integration with go2rtc. The application does not sanitize user input in the video stream configuration (config.yaml), allowing direct injection of system commands via the exec: directive. The go2rtc service executes these commands without restrictions. This vulnerability is only exploitable by an administrator or users who have exposed their Frigate install to the open internet with no authentication which allows anyone full administrative control. This vulnerability is fixed in 0.16.4.	9.1	More Details

CVE-2026-24679	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.22.0, The URBDRC client uses server-supplied interface numbers as array indices without bounds checks, causing an out-of-bounds read in libusb_udev_select_interface. This vulnerability is fixed in 3.22.0.	9.1	More Details
CVE-2026-24677	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.22.0, ecam_encoder_compress_h264 trusts server-controlled dimensions and does not validate the source buffer size, leading to an out-of-bounds read in sws_scale. This vulnerability is fixed in 3.22.0.	9.1	More Details
CVE-2026-25848	In JetBrains Hub before 2025.3.119807 authentication bypass allowing administrative actions was possible	9.1	More Details
CVE-2026-25160	Alist is a file list program that supports multiple storages, powered by Gin and Solidjs. Prior to version 3.57.0, the application disables TLS certificate verification by default for all outgoing storage driver communications, making the system vulnerable to Man-in-the-Middle (MitM) attacks. This enables the complete decryption, theft, and manipulation of all data transmitted during storage operations, severely compromising the confidentiality and integrity of user data. This issue has been patched in version 3.57.0.	9.1	More Details
CVE-2026-25722	Claude Code is an agentic coding tool. Prior to version 2.0.57, Claude Code failed to properly validate directory changes when combined with write operations to protected folders. By using the cd command to navigate into sensitive directories like .claude, it was possible to bypass write protection and create or modify files without user confirmation. Reliably exploiting this required the ability to add untrusted content into a Claude Code context window. This issue has been patched in version 2.0.57.	9.1	More Details
CVE-2026-25752	FUXA is a web-based Process Visualization (SCADA/HMI/Dashboard) software. An authorization bypass vulnerability in FUXA allows an unauthenticated, remote attacker to modify device tags via WebSockets. Exploitation allows an unauthenticated, remote attacker to bypass role-based access controls and overwrite arbitrary device tags or disable communication drivers, exposing connected ICS/SCADA environments to follow-on actions. This may allow an attacker to manipulate physical processes and disconnected devices from the HMI. This affects FUXA through version 1.2.9. This issue has been patched in FUXA version 1.2.10.	9.1	More Details
CVE-2026-2234	C&Cm@il developed by HGiga has a Missing Authentication vulnerability, allowing unauthenticated remote attackers to read and modify any user's mail content.	9.1	More Details
CVE-2026-25881	SandboxJS is a JavaScript sandboxing library. Prior to 0.8.31, a sandbox escape vulnerability allows sandboxed code to mutate host built-in prototypes by laundering the isGlobal protection flag through array literal intermediaries. When a global prototype reference (e.g., Map.prototype, Set.prototype) is placed into an array and retrieved, the isGlobal taint is stripped, permitting direct prototype mutation from within the sandbox. This results in persistent host-side prototype pollution and may enable RCE in applications that use polluted properties in sensitive sinks (example gadget: execSync(obj.cmd)). This vulnerability is fixed in 0.8.31.	9.0	More Details
CVE-2025-68723	Axigen Mail Server before 10.5.57 contains multiple stored Cross-Site Scripting (XSS) vulnerabilities in the WebAdmin interface. Three instances exist: (1) the log file name parameter in the Local Services Log page, (2) certificate file content in the SSL Certificates View Usage feature, and (3) the Certificate File name parameter in the WebMail Listeners SSL settings. Attackers can inject malicious JavaScript payloads that execute in administrators' browsers when they access affected pages or features, enabling privilege escalation attacks where low-privileged admins can force high-privileged admins to perform unauthorized actions.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2026-23687	SAP NetWeaver Application Server ABAP and ABAP Platform allows an authenticated attacker with normal privileges to obtain a valid signed message and send modified signed XML documents to the verifier. This may result in acceptance of tampered identity information, unauthorized access to sensitive user data and potential disruption of normal system usage.	8.8	More Details
CVE-2025-10314	Incorrect Default Permissions vulnerability in Mitsubishi Electric Corporation FREQSHIP-mini for Windows versions 8.0.0 to 8.0.2 allows a local attacker to execute arbitrary code with system privileges by replacing service executable files (EXE) or DLLs in the installation directory with specially crafted files. As a result, the attacker may be able to disclose, tamper with, delete, or destroy information stored on the PC where the affected product is installed, or cause a Denial of Service (DoS) condition on the affected system.	8.8	More Details
CVE-2026-25859	Wekan versions prior to 8.20 allow non-administrative users to access migration functionality due to insufficient permission checks, potentially resulting in unauthorized migration operations.	8.8	More Details
CVE-2026-25947	Worklenz is a project management tool. Prior to 2.1.7, there are multiple SQL injection vulnerabilities were discovered in backend SQL query construction affecting project and task management controllers, reporting and financial data endpoints, real-time socket.io handlers, and resource allocation and scheduling features. The vulnerability has been patched in version v2.1.7.	8.8	More Details
CVE-2025-15100	The JAY Login & Register plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 2.6.03. This is due to the plugin allowing a user to update arbitrary user meta through the 'jay_panel_ajax_update_profile' function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to elevate their privileges to that of an administrator.	8.8	More Details
CVE-2025-15368	The SportsPress plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 2.7.26 via shortcodes 'template_name' attribute. This makes it possible for authenticated attackers, with contributor-level and above permissions, to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where php file type can be uploaded and included.	8.8	More Details
CVE-2026-21537	Improper control of generation of code ('code injection') in Microsoft Defender for Linux allows an unauthorized attacker to execute code over an adjacent network.	8.8	More Details
CVE-2026-2137	A vulnerability has been found in Tenda TX3 up to 16.03.13.11_multi. This impacts an unknown function of the file /goform/SetIpMacBind. The manipulation of the argument list leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2026-2138	A vulnerability was found in Tenda TX9 up to 22.03.02.10_multi. Affected is the function sub_42D03C of the file /goform/SetStaticRouteCfg. The manipulation of the argument list results in buffer overflow. The attack can be launched remotely. The exploit has been made public and could be used.	8.8	More Details
CVE-2026-2139	A vulnerability was determined in Tenda TX9 up to 22.03.02.10_multi. Affected by this vulnerability is the function sub_432580 of the file /goform/fast_setting_wifi_set. This manipulation of the argument ssid causes buffer overflow. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized.	8.8	More Details
CVE-2026-25056	n8n is an open source workflow automation platform. Prior to versions 1.118.0 and 2.4.0, a vulnerability in the Merge node's SQL Query mode allowed authenticated users with permission to create or modify workflows to write arbitrary files to the n8n server's filesystem potentially leading to remote code execution. This issue has been patched in versions 1.118.0 and 2.4.0.	8.8	More Details
	A weakness has been identified in UTT 进取 520W 1.7.7-180627. This affects the function		

CVE-2026-2066	strcpy of the file /goform/formIpGroupConfig. Executing a manipulation of the argument groupName can lead to buffer overflow. The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2026-2067	A security vulnerability has been detected in UTT 进取 520W 1.7.7-180627. This vulnerability affects the function strcpy of the file /goform/formTimeGroupConfig. The manipulation of the argument year1 leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2026-21516	Improper neutralization of special elements used in a command ('command injection') in Github Copilot allows an unauthorized attacker to execute code over a network.	8.8	More Details
CVE-2026-21513	Protection mechanism failure in MSHTML Framework allows an unauthorized attacker to bypass a security feature over a network.	8.8	More Details
CVE-2026-2071	A vulnerability was found in UTT 进取 520W 1.7.7-180627. The impacted element is the function strcpy of the file /goform/formP2PLimitConfig. Performing a manipulation of the argument except results in buffer overflow. The attack is possible to be carried out 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.	8.8	More Details
CVE-2026-2140	A vulnerability was identified in Tenda TX9 up to 22.03.02.10_multi. Affected by this issue is the function sub_4223E0 of the file /goform/setMacFilterCfg. Such manipulation of the argument deviceList leads to buffer overflow. The attack may be launched remotely. The exploit is publicly available and might be used.	8.8	More Details
CVE-2026-21510	Protection mechanism failure in Windows Shell allows an unauthorized attacker to bypass a security feature over a network.	8.8	More Details
CVE-2026-1486	A flaw was found in Keycloak. A vulnerability exists in the jwt-authorization-grant flow where the server fails to verify if an Identity Provider (IdP) is enabled before issuing tokens. The issuer lookup mechanism (lookupIdentityProviderFromIssuer) retrieves the IdP configuration but does not filter for isEnabled=false. If an administrator disables an IdP (e.g., due to a compromise or offboarding), an entity possessing that IdP's signing key can still generate valid JWT assertions that Keycloak accepts, resulting in the issuance of valid access tokens.	8.8	More Details
CVE-2025-69906	Monstra CMS v3.0.4 contains an arbitrary file upload vulnerability in the Files Manager plugin. The application relies on blacklist-based file extension validation and stores uploaded files directly in a web-accessible directory. Under typical server configurations, this can allow an attacker to upload files that are interpreted as executable code, resulting in remote code execution.	8.8	More Details
CVE-2026-2070	A vulnerability has been found in UTT 进取 520W 1.7.7-180627. The affected element is the function strcpy of the file /goform/formPolicyRouteConf. Such manipulation of the argument GroupName leads to buffer overflow. The attack can be executed remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2026-2094	Docpedia developed by Flowring has a SQL Injection vulnerability, allowing authenticated remote attackers to inject arbitrary SQL commands to read, modify, and delete database contents.	8.8	More Details
CVE-2026-2097	Agentflow developed by Flowring has an Arbitrary File Upload vulnerability, allowing authenticated remote attackers to upload and execute web shell backdoors, thereby enabling arbitrary code execution on the server.	8.8	More Details
CVE-2025-10465	Unrestricted Upload of File with Dangerous Type vulnerability in Birtech Information Technologies Industry and Trade Ltd. Co. Sensaway allows Upload a Web Shell to a Web Server.This issue affects Sensaway: through 09022026. NOTE: The vendor was contacted	8.8	More Details

	early about this disclosure but did not respond in any way.		
CVE-2026-25161	Alist is a file list program that supports multiple storages, powered by Gin and Solidjs. Prior to version 3.57.0, the application contains path traversal vulnerability in multiple file operation handlers. An authenticated attacker can bypass directory-level authorisation by injecting traversal sequences into filename components, enabling unauthorised file removal, movement and copying across user boundaries within the same storage mount. This issue has been patched in version 3.57.0.	8.8	More Details
CVE-2025-15566	A security issue was discovered in ingress-nginx where the `nginx.ingress.kubernetes.io/auth-proxy-set-headers` Ingress annotation can be used to inject configuration into nginx. This can lead to arbitrary code execution in the context of the ingress-nginx controller, and disclosure of Secrets accessible to the controller. (Note that in the default installation, the controller can access all Secrets cluster-wide.)	8.8	More Details
CVE-2026-21255	Improper access control in Windows Hyper-V allows an authorized attacker to bypass a security feature locally.	8.8	More Details
CVE-2026-21256	Improper neutralization of special elements used in a command ('command injection') in GitHub Copilot and Visual Studio allows an unauthorized attacker to execute code over a network.	8.8	More Details
CVE-2026-20098	A vulnerability in the Certificate Management feature of Cisco Meeting Management could allow an authenticated, remote attacker to upload arbitrary files, execute arbitrary commands, and elevate privileges to root on an affected system. This vulnerability is due to improper input validation in certain sections of the web-based management interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected system. A successful exploit could allow the attacker to upload arbitrary files to the affected system. The malicious files could overwrite system files that are processed by the root system account and allow arbitrary command execution with root privileges. To exploit this vulnerability, the attacker must have valid credentials for a user account with at least the role of video operator.	8.8	More Details
CVE-2026-24343	Improper Neutralization of Data within XPath Expressions ('XPath Injection') vulnerability in Apache HertzBeat. This issue affects Apache HertzBeat: from 1.7.1 before 1.8.0. Users are recommended to upgrade to version 1.8.0, which fixes the issue.	8.8	More Details
CVE-2025-68722	Axigen Mail Server before 10.5.57 and 10.6.x before 10.6.26 contains a Cross-Site Request Forgery (CSRF) vulnerability in the WebAdmin interface through improper handling of the _s (breadcrumb) parameter. The application accepts state-changing requests via the GET method and automatically processes base64-encoded commands queued in the _s parameter immediately after administrator authentication. Attackers can craft malicious URLs that, when clicked by administrators, execute arbitrary administrative actions upon login without further user interaction, including creating rogue administrator accounts or modifying critical server configurations.	8.8	More Details
CVE-2026-2181	A security flaw has been discovered in Tenda RX3 16.03.13.11. Affected by this vulnerability is an unknown functionality of the file /goform/openSchedWifi. Performing a manipulation of the argument schedStartTime/schedEndTime results in stack-based buffer overflow. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks.	8.8	More Details
CVE-2026-2180	A vulnerability was identified in Tenda RX3 16.03.13.11. Affected is an unknown function of the file /goform/fast_setting_wifi_set. Such manipulation of the argument ssid_5g leads to stack-based buffer overflow. The attack can be launched remotely. The exploit is publicly available and might be used.	8.8	More Details
CVE-2025-7347	Authorization Bypass Through User-Controlled Key vulnerability in Dinibh Puzzle Software Solutions Dinibh Patrol Tracking System allows Exploitation of Trusted Identifiers.This issue affects Dinibh Patrol Tracking System: through 10022026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
	A vulnerability has been found in Tenda RX3 16.03.13.11. Impacted is the function		

CVE-2026-2186	fromSetIpMacBind of the file /goform/SetIpMacBind. Such manipulation of the argument list leads to stack-based buffer overflow. The attack may be performed from remote. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2025-69214	OpenSTAManager is an open source management software for technical assistance and invoicing. In 2.9.8 and earlier, an SQL Injection vulnerability exists in the ajax_select.php endpoint when handling the componenti operation. An authenticated attacker can inject malicious SQL code through the options[matricola] parameter.	8.8	More Details
CVE-2025-69212	OpenSTAManager is an open source management software for technical assistance and invoicing. In 2.9.8 and earlier, a critical OS Command Injection vulnerability exists in the P7M (signed XML) file decoding functionality. An authenticated attacker can upload a ZIP file containing a .p7m file with a malicious filename to execute arbitrary system commands on the server.	8.8	More Details
CVE-2026-1756	The WP FOFT Loader plugin for WordPress is vulnerable to arbitrary file uploads due to incorrect file type validation in the 'WP_FOFT_Loader_Mimes::file_and_ext' function in all versions up to, and including, 2.1.39. This makes it possible for authenticated attackers, with Author-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	8.8	More Details
CVE-2026-2086	A vulnerability was detected in UTT HiPER 810G up to 1.7.7-171114. Affected by this vulnerability is the function strcpy of the file /goform/formFireWall of the component Management Interface. The manipulation of the argument GroupName results in buffer overflow. The attack can 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 any way.	8.8	More Details
CVE-2026-2068	A vulnerability was detected in UTT 进取 520W 1.7.7-180627. This issue affects the function strcpy of the file /goform/formSyslogConf. The manipulation of the argument ServerIp results in buffer overflow. 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 any way.	8.8	More Details
CVE-2026-2203	A flaw has been found in Tenda AC8 16.03.33.05. Affected by this vulnerability is an unknown functionality of the file /goform/fast_setting_wifi_set of the component Embedded Httpd Service. This manipulation of the argument timeZone causes buffer overflow. Remote exploitation of the attack is possible. The exploit has been published and may be used.	8.8	More Details
CVE-2026-2202	A vulnerability was detected in Tenda AC8 16.03.33.05. Affected is the function fromSetWifiGusetBasic of the file /goform/WifiGuestSet of the component httpd. The manipulation of the argument shareSpeed results in buffer overflow. The attack may be launched remotely. The exploit is now public and may be used.	8.8	More Details
CVE-2025-15330	Tanium addressed an improper input validation vulnerability in Deploy.	8.8	More Details
CVE-2026-25761	Super-linter is a combination of multiple linters to run as a GitHub Action or standalone. From 6.0.0 to 8.3.0, the Super-linter GitHub Action is vulnerable to command injection via crafted filenames. When this action is used in downstream GitHub Actions workflows, an attacker can submit a pull request that introduces a file whose name contains shell command substitution syntax, such as $(...). In affected Super-linter versions, runtime scripts may execute the embedded command during file discovery processing, enabling arbitrary command execution in the workflow runner context. This can be used to disclose the job's GITHUB_TOKEN depending on how the workflow configures permissions. This vulnerability is fixed in 8.3.1.	8.8	More Details
CVE-2026-20841	Improper neutralization of special elements used in a command ('command injection') in Windows Notepad App allows an unauthorized attacker to execute code over a network.	8.8	More Details
CVE-2026-	A vulnerability was found in Tenda RX3 16.03.13.11. The affected element is the function set_qosMib_list of the file /goform/formSetQosBand. Performing a manipulation of the argument list results in stack-based buffer overflow. It is possible to initiate the attack	8.8	More Details

2187	argument list results in stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been made public and could be used.		Details
CVE-2026-1819	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Karel Electronics Industry and Trade Inc. ViPort allows Stored XSS.This issue affects ViPort: through 23012026.	8.8	More Details
CVE-2026-25807	ZAI Shell is an autonomous SysOps agent designed to navigate, repair, and secure complex environments. Prior to 9.0.3, the P2P terminal sharing feature (share start) opens a TCP socket on port 5757 without any authentication mechanism. Any remote attacker can connect to this port using a simple socket script. An attacker who connects to a ZAI-Shell P2P session running in --no-ai mode can send arbitrary system commands. If the host user approves the command without reviewing its contents, the command executes directly with the user's privileges, bypassing all Sentinel safety checks. This vulnerability is fixed in 9.0.3.	8.8	More Details
CVE-2020-37117	jizhiCMS 1.6.7 contains a file download vulnerability in the admin plugins update endpoint that allows authenticated administrators to download arbitrary files. Attackers can exploit the vulnerability by sending crafted POST requests with malicious filepath and download_url parameters to trigger unauthorized file downloads.	8.8	More Details
CVE-2025-7636	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Ergosis Security Systems Computer Industry and Trade Inc. ZEUS PDKS allows SQL Injection.This issue affects ZEUS PDKS: from <1.0.5.10 through 10022026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2025-52436	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability [CWE-79] vulnerability in Fortinet FortiSandbox 5.0.0 through 5.0.1, FortiSandbox 4.4.0 through 4.4.7, FortiSandbox 4.2 all versions, FortiSandbox 4.0 all versions may allow an unauthenticated attacker to execute commands via crafted requests.	8.8	More Details
CVE-2026-2185	A flaw has been found in Tenda RX3 16.03.13.11. This issue affects the function set_device_name of the file /goform/setBlackRule of the component MAC Filtering Configuration Endpoint. This manipulation of the argument devName/mac causes stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit has been published and may be used.	8.8	More Details
CVE-2025-6967	Execution After Redirect (EAR) vulnerability in Sarman Soft Software and Technology Services Industry and Trade Ltd. Co. CMS allows JSON Hijacking (aka JavaScript Hijacking), Authentication Bypass.This issue affects CMS: through 10022026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.7	More Details
CVE-2026-25580	Pydantic AI is a Python agent framework for building applications and workflows with Generative AI. From 0.0.26 to before 1.56.0, aServer-Side Request Forgery (SSRF) vulnerability exists in Pydantic AI's URL download functionality. When applications accept message history from untrusted sources, attackers can include malicious URLs that cause the server to make HTTP requests to internal network resources, potentially accessing internal services or cloud credentials. This vulnerability only affects applications that accept message history from external users. This vulnerability is fixed in 1.56.0.	8.6	More Details
CVE-2025-7799	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Zirve Information Technologies Inc. E-Taxpayer Accounting Website allows Reflected XSS.This issue affects e-Taxpayer Accounting Website: through 07082025.	8.6	More Details
CVE-2025-32008	Out-of-bounds write in the firmware for the Intel(R) AMT and Intel(R) Standard Manageability within Ring 3: User Applications may allow a denial of service. Network adversary with an unauthenticated user combined with a low complexity attack may enable denial of service. This result may potentially occur via network access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (none), integrity (none) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (low) impacts.	8.6	More Details
CVE-2025-	IBM Aspera Console 3.4.0 through 3.4.8 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add,	8.6	More

13379	modify, or delete information in the back-end database.		Details
CVE-2026-25635	calibre is an e-book manager. Prior to 9.2.0, Calibre's CHM reader contains a path traversal vulnerability that allows arbitrary file writes anywhere the user has write permissions. On Windows (haven't tested on other OS's), this can lead to Remote Code Execution by writing a payload to the Startup folder, which executes on next login. This vulnerability is fixed in 9.2.0.	8.6	More Details
CVE-2026-24302	Azure Arc Elevation of Privilege Vulnerability	8.6	More Details
CVE-2025-61732	A discrepancy between how Go and C/C++ comments were parsed allowed for code smuggling into the resulting cgo binary.	8.6	More Details
CVE-2026-1603	An authentication bypass in Ivanti Endpoint Manager before version 2024 SU5 allows a remote unauthenticated attacker to leak specific stored credential data.	8.6	More Details
CVE-2026-25628	Qdrant is a vector similarity search engine and vector database. From 1.9.3 to before 1.16.0, it is possible to append to arbitrary files via /logger endpoint using an attacker-controlled on_disk.log_file path. Minimal privileges are required (read-only access). This vulnerability is fixed in 1.16.0.	8.5	More Details
CVE-2020-37139	Odin Secure FTP Expert 7.6.3 contains a local denial of service vulnerability that allows attackers to crash the application by manipulating site information fields. Attackers can generate a buffer overflow by pasting 108 bytes of repeated characters into connection fields, causing the application to crash.	8.4	More Details
CVE-2026-24930	UAF concurrency vulnerability in the graphics module. Impact: Successful exploitation of this vulnerability may affect availability.	8.4	More Details
CVE-2026-24884	Compressing is a compressing and uncompressing lib for node. In version 2.0.0 and 1.10.3 and prior, Compressing extracts TAR archives while restoring symbolic links without validating their targets. By embedding symlinks that resolve outside the intended extraction directory, an attacker can cause subsequent file entries to be written to arbitrary locations on the host file system. Depending on the extractor’s handling of existing files, this behavior may allow overwriting sensitive files or creating new files in security-critical locations. This issue has been patched in versions 1.10.4 and 2.0.1.	8.4	More Details
CVE-2026-25593	OpenClaw is a personal AI assistant. Prior to 2026.1.20, an unauthenticated local client could use the Gateway WebSocket API to write config via config.apply and set unsafe cliPath values that were later used for command discovery, enabling command injection as the gateway user. This vulnerability is fixed in 2026.1.20.	8.4	More Details
CVE-2026-24926	Out-of-bounds write vulnerability in the camera module. Impact: Successful exploitation of this vulnerability may affect availability.	8.4	More Details
CVE-2020-37142	10-Strike Network Inventory Explorer 8.54 contains a structured exception handler buffer overflow vulnerability that allows attackers to execute arbitrary code by overwriting SEH records. Attackers can craft a malicious payload targeting the 'Computer' parameter during the 'Add' function to trigger remote code execution.	8.4	More Details
CVE-2026-25847	In JetBrains PyCharm before 2025.3.2 a DOM-based XSS on Jupyter viewer page was possible	8.2	More Details
CVE-2026-25636	calibre is an e-book manager. In 9.1.0 and earlier, a path traversal vulnerability in Calibre's EPUB conversion allows a malicious EPUB file to corrupt arbitrary existing files writable by the Calibre process. During conversion, Calibre resolves CipherReference URI from META-INF/encryption.xml to an absolute filesystem path and opens it in read-write mode, even	8.2	More Details

	when it points outside the conversion extraction directory. This vulnerability is fixed in 9.2.0.		
CVE-2026-21532	Azure Function Information Disclosure Vulnerability	8.2	More Details
CVE-2025-25210	Improper input validation for some Server Firmware Update Utility(SysFwUpdt) before version 16.0.12 within Ring 3: User Applications may allow an escalation of privilege. System software adversary with a privileged user combined with a low complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	8.2	More Details
CVE-2025-59023	Crafted delegations or IP fragments can poison cached delegations in Recursor.	8.2	More Details
CVE-2025-13192	The Popup builder with Gamification, Multi-Step Popups, Page-Level Targeting, and WooCommerce Triggers plugin for WordPress is vulnerable to generic SQL Injection via the multiple REST API endpoints in all versions up to, and including, 2.2.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. Vulnerability was patched in version 2.2.1 for unauthenticated users, and fully patched in version 2.2.3 for Administrator+ level users.	8.2	More Details
CVE-2026-24843	melange allows users to build apk packages using declarative pipelines. In version 0.11.3 to before 0.40.3, an attacker who can influence the tar stream from a QEMU guest VM could write files outside the intended workspace directory on the host. The retrieveWorkspace function extracts tar entries without validating that paths stay within the workspace, allowing path traversal via ../ sequences. This issue has been patched in version 0.40.3.	8.2	More Details
CVE-2020-37151	phpMyChat Plus 1.98 contains a SQL injection vulnerability in the deluser.php page through the pmc_username parameter that allows attackers to manipulate database queries. Attackers can exploit boolean-based, error-based, and time-based blind SQL injection techniques to extract sensitive database information by crafting malicious payloads in the username field.	8.2	More Details
CVE-2020-37163	QuickDate 1.3.2 contains a SQL injection vulnerability that allows remote attackers to manipulate database queries through the '_located' parameter in the find_matches endpoint. Attackers can inject UNION-based SQL statements to extract database information including user credentials, database name, and system version.	8.2	More Details
CVE-2026-23989	REVA is an interoperability platform. Prior to 2.42.3 and 2.40.3, a bug in the GRPC authorization middleware of the "Reva" component of OpenCloud allows a malicious user to bypass the scope verification of a public link. By exploiting this via the the "archiver" service this can be leveraged to create an archive (zip or tar-file) containing all resources that this creator of the public link has access to. This vulnerability is fixed in 2.42.3 and 2.40.3.	8.2	More Details
CVE-2020-37141	AMSS++ version 4.31 contains a SQL injection vulnerability in the mail module's maildetail.php script through the 'id' parameter. Attackers can manipulate the 'id' parameter in /modules/mail/main/maildetail.php to inject malicious SQL queries and potentially access or modify database contents.	8.2	More Details
CVE-2020-37149	Edimax EW-7438RPn-v3 Mini 1.27 is vulnerable to cross-site request forgery (CSRF) that can lead to command execution. An attacker can trick an authenticated user into submitting a crafted form to the /goform/mp endpoint, resulting in arbitrary command execution on the device with the user's privileges.	8.1	More Details
CVE-2026-	An Authentication Bypass by Primary Weakness vulnerability [CWE-305] vulnerability in Fortinet FortiOS 7.6.0 through 7.6.4 may allow an unauthenticated attacker to bypass LDAP	8.1	More

22153	authentication of Agentless VPN or FSSO policy, when the remote LDAP server is configured in a specific way.		Details
CVE-2026-25055	n8n is an open source workflow automation platform. Prior to versions 1.123.12 and 2.4.0, when workflows process uploaded files and transfer them to remote servers via the SSH node without validating their metadata the vulnerability can lead to files being written to unintended locations on those remote systems potentially leading to remote code execution on those systems. As a prerequisites an unauthenticated attacker needs knowledge of such workflows existing and the endpoints for file uploads need to be unauthenticated. This issue has been patched in versions 1.123.12 and 2.4.0.	8.1	More Details
CVE-2026-21228	Improper certificate validation in Azure Local allows an unauthorized attacker to execute code over a network.	8.1	More Details
CVE-2026-25519	OpenSlides is a free, web based presentation and assembly system for managing and projecting agenda, motions and elections of an assembly. Prior to version 4.2.29, OpenSlides supports local logins with username and password or an optionally configurable single sign on with SAML via an external IDP. For users synced to OpenSlides via an external IDP, there is an incorrect access control regarding the local login of these users. Users can successfully login using the local login form and the OpenSlides username of a SAML user and a trivial password. This password is valid for all SAML users. This issue has been patched in version 4.2.29.	8.1	More Details
CVE-2026-25890	File Browser provides a file managing interface within a specified directory and it can be used to upload, delete, preview, rename and edit files. Prior to 2.57.1, an authenticated user can bypass the application's "Disallow" file path rules by modifying the request URL. By adding multiple slashes (e.g., //private/) to the path, the authorization check fails to match the rule, while the underlying filesystem resolves the path correctly, granting unauthorized access to restricted files. This vulnerability is fixed in 2.57.1.	8.1	More Details
CVE-2025-68721	Axigen Mail Server before 10.5.57 contains an improper access control vulnerability in the WebAdmin interface. A delegated admin account with zero permissions can bypass access control checks and gain unauthorized access to the SSL Certificates management endpoint (page=sslcerts). This allows the attacker to view, download, upload, and delete SSL certificate files, despite lacking the necessary privileges to access the Security & Filtering section.	8.1	More Details
CVE-2026-22038	AutoGPT is a platform that allows users to create, deploy, and manage continuous artificial intelligence agents that automate complex workflows. Prior to autogpt-platform-beta-v0.6.46, the AutoGPT platform's Stagehand integration blocks log API keys and authentication secrets in plaintext using logger.info() statements. This occurs in three separate block implementations (StagehandObserveBlock, StagehandActBlock, and StagehandExtractBlock) where the code explicitly calls api_key.get_secret_value() and logs the result. This issue has been patched in autogpt-platform-beta-v0.6.46.	8.1	More Details
CVE-2026-1529	A flaw was found in Keycloak. An attacker can exploit this vulnerability by modifying the organization ID and target email within a legitimate invitation token's JSON Web Token (JWT) payload. This lack of cryptographic signature verification allows the attacker to successfully self-register into an unauthorized organization, leading to unauthorized access.	8.1	More Details
CVE-2026-21229	Improper input validation in Power BI allows an authorized attacker to execute code over a network.	8.0	More Details
CVE-2026-21257	Improper neutralization of special elements used in a command ('command injection') in GitHub Copilot and Visual Studio allows an authorized attacker to elevate privileges over a network.	8.0	More Details
CVE-2026-21523	Time-of-check time-of-use (toctou) race condition in GitHub Copilot and Visual Studio allows an authorized attacker to execute code over a network.	8.0	More Details

CVE-2025-30513	Race condition for some TDX Module within Ring 0: Hypervisor may allow an escalation of privilege. System software adversary with a privileged user combined with a low complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are not present with special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (none) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	7.9	More Details
CVE-2026-24844	melange allows users to build apk packages using declarative pipelines. From version 0.3.0 to before 0.40.3, an attacker who can provide build input values, but not modify pipeline definitions, could execute arbitrary shell commands if the pipeline uses ${{vars.*}} or ${{inputs.*}} substitutions in working-directory. The field is embedded into shell scripts without proper quote escaping. This issue has been patched in version 0.40.3.	7.9	More Details
CVE-2025-35998	Missing protection mechanism for alternate hardware interface in the Intel(R) Quick Assist Technology for some Intel(R) Platforms within Ring 0: Kernel may allow an escalation of privilege. System software adversary with a privileged user combined with a low complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are present with special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (none) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	7.9	More Details
CVE-2019-25285	Alps Pointing-device Controller 8.1202.1711.04 contains an unquoted service path vulnerability in the ApHidMonitorService that allows local attackers to execute code with elevated privileges. Attackers can place a malicious executable in the service path and gain system-level access when the service restarts or the system reboots.	7.8	More Details
CVE-2026-25582	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of ICC color management profiles. Prior to version 2.3.1.3, there is a heap buffer overflow (read) vulnerability in CIccIO::WriteUInt16Float() when converting malformed XML to ICC profiles via iccFromXml tool. This issue has been patched in version 2.3.1.3.	7.8	More Details
CVE-2026-25583	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of ICC color management profiles. Prior to version 2.3.1.3, there is a heap buffer overflow vulnerability in CIccFileIO::Read8() when processing malformed ICC profile files via unchecked fread operation. This issue has been patched in version 2.3.1.3.	7.8	More Details
CVE-2026-25584	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of ICC color management profiles. Prior to version 2.3.1.3, there is a stack-buffer-overflow vulnerability in CIccTagFloatNum<>::GetValues(). This is triggered when processing a malformed ICC profile. The vulnerability allows an out-of-bounds write on the stack, potentially leading to memory corruption, information disclosure, or code execution when processing specially crafted ICC files. This issue has been patched in version 2.3.1.3.	7.8	More Details
CVE-2019-25276	Studio 5000 Logix Designer 30.01.00 contains an unquoted service path vulnerability in the FactoryTalk Activation Service that allows local users to potentially execute code with elevated privileges. Attackers can exploit the unquoted path in C:\Program Files (x86)\Rockwell Software\FactoryTalk Activation\ to inject malicious code that would execute with LocalSystem permissions.	7.8	More Details
CVE-2019-25283	Shrew Soft VPN Client 2.2.2 contains an unquoted service path vulnerability that allows local users to execute arbitrary code with elevated system privileges. Attackers can place malicious executables in the unquoted service path to gain elevated access during service startup or system reboot.	7.8	More Details
CVE-2019-25281	NCP Secure Entry Client 9.2 contains an unquoted service path vulnerability in multiple Windows services that allows local users to potentially execute arbitrary code. Attackers can exploit the unquoted paths in services like ncprwsnt, rwsrsu, ncpclcfg, and NcpSec to inject malicious code that would execute with LocalSystem privileges during service startup.	7.8	More Details
CVE-	Adaware Web Companion version 4.8.2078.3950 contains an unquoted service path vulnerability in the WCAssistantService that allows local users to potentially execute code		

2019-25287	with elevated privileges. Attackers can exploit the unquoted path in C:\Program Files (x86)\Lavasoft\Web Companion\Application\ to inject malicious code that would execute with LocalSystem privileges during service startup.	7.8	More Details
CVE-2019-25274	ProShow Producer 9.0.3797 contains an unquoted service path vulnerability in the ScsiAccess service that allows local attackers to potentially execute arbitrary code. Attackers can exploit the unquoted binary path to inject malicious executables that will be run with LocalSystem privileges during service startup.	7.8	More Details
CVE-2026-25585	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of ICC color management profiles. Prior to version 2.3.1.3, there is a vulnerability IccCmm.cpp:5793 when reading through index during ICC profile processing. The malformed ICC profile triggers improper array bounds validation in the color management module, resulting in an out-of-bounds read that can lead to memory disclosure or segmentation fault from accessing memory beyond the array boundary. This issue has been patched in version 2.3.1.3.	7.8	More Details
CVE-2019-25267	Wing FTP Server 6.0.7 contains an unquoted service path vulnerability that allows local attackers to potentially execute arbitrary code with elevated system privileges. Attackers can exploit the unquoted binary path in the service configuration to inject malicious executables that will be launched with LocalSystem permissions.	7.8	More Details
CVE-2019-25269	Amiti Antivirus 25.0.640 contains an unquoted service path vulnerability in its Windows service configurations. Attackers can exploit the unquoted path to inject and execute malicious code with elevated LocalSystem privileges by placing executable files in specific directory locations.	7.8	More Details
CVE-2019-25271	NETGATE Data Backup 3.0.620 contains an unquoted service path vulnerability in its NGDatBckpSrv Windows service configuration. Attackers can exploit the unquoted path to inject and execute malicious code with LocalSystem privileges by placing executable files in specific directory locations.	7.8	More Details
CVE-2019-25286	GCafé 3.0 contains an unquoted service path vulnerability in the gbClientService that allows local attackers to potentially execute arbitrary code with elevated privileges. Attackers can exploit the unquoted path in the service configuration to inject malicious executables that will be run with LocalSystem permissions.	7.8	More Details
CVE-2026-23717	A vulnerability has been identified in Simcenter Femap (All versions < V2512), Simcenter Nastran (All versions < V2512). The affected applications contains an out of bounds read vulnerability while parsing specially crafted XDB files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2026-25546	Godot MCP is a Model Context Protocol (MCP) server for interacting with the Godot game engine. Prior to version 0.1.1, a command injection vulnerability in godot-mcp allows remote code execution. The executeOperation function passed user-controlled input (e.g., projectPath) directly to exec(), which spawns a shell. An attacker could inject shell metacharacters like $(command) or &calc to execute arbitrary commands with the privileges of the MCP server process. This affects any tool that accepts projectPath, including create_scene, add_node, load_sprite, and others. This issue has been patched in version 0.1.1.	7.8	More Details
CVE-2026-25880	SumatraPDF is a multi-format reader for Windows. In 3.5.2 and earlier, the PDF reader allows execution of a malicious binary (explorer.exe) located in the same directory as the opened PDF when the user clicks File → “Show in folder”. This behavior leads to arbitrary code execution on the victim’s system with the privileges of the current user, without any warning or user interaction beyond the menu click.	7.8	More Details
CVE-2026-23718	A vulnerability has been identified in Simcenter Femap (All versions < V2512), Simcenter Nastran (All versions < V2512). The affected applications contains an out of bounds read vulnerability while parsing specially crafted NDB files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-	A vulnerability has been identified in Simcenter Femap (All versions < V2512), Simcenter Nastran (All versions < V2512). The affected application is vulnerable to heap-based buffer		More

2026-23719	Nastran (All versions < V2512). The affected application is vulnerable to heap-based buffer overflow while parsing specially crafted NDB files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2026-23720	A vulnerability has been identified in Simcenter Femap (All versions < V2512), Simcenter Nastran (All versions < V2512). The affected applications contains an out of bounds read vulnerability while parsing specially crafted NDB files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2026-25655	A vulnerability has been identified in SINEC NMS (All versions < V4.0 SP2). The affected application permits improper modification of a configuration file by a low-privileged user. This could allow an attacker to load malicious DLLs, potentially leading to arbitrary code execution with administrative privilege.(ZDI-CAN-28107)	7.8	More Details
CVE-2026-25143	melange allows users to build apk packages using declarative pipelines. From version 0.10.0 to before 0.40.3, an attacker who can influence inputs to the patch pipeline could execute arbitrary shell commands on the build host. The patch pipeline in pkg/build/pipelines/patch.yaml embeds input-derived values (series paths, patch filenames, and numeric parameters) into shell scripts without proper quoting or validation, allowing shell metacharacters to break out of their intended context. The vulnerability affects the built-in patch pipeline which can be invoked through melange build and melange license-check operations. An attacker who can control patch-related inputs (e.g., through pull request-driven CI, build-as-a-service, or by influencing melange configurations) can inject shell metacharacters such as backticks, command substitutions $(...), semicolons, pipes, or redirections to execute arbitrary commands with the privileges of the melange build process. This issue has been patched in version 0.40.3.	7.8	More Details
CVE-2026-23716	A vulnerability has been identified in Simcenter Femap (All versions < V2512), Simcenter Nastran (All versions < V2512). The affected applications contains an out of bounds read vulnerability while parsing specially crafted XDB files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2026-25656	A vulnerability has been identified in SINEC NMS (All versions), User Management Component (UMC) (All versions < V2.15.2.1). The affected application permits improper modification of a configuration file by a low-privileged user. This could allow an attacker to load malicious DLLs, potentially leading to arbitrary code execution with SYSTEM privileges. (ZDI-CAN-28108)	7.8	More Details
CVE-2026-23715	A vulnerability has been identified in Simcenter Femap (All versions < V2512), Simcenter Nastran (All versions < V2512). The affected applications contains an out of bounds write vulnerability while parsing specially crafted XDB files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2026-22923	A vulnerability has been identified in NX (All versions < V2512). The affected application contains a data validation vulnerability that could allow an attacker with local access to interfere with internal data during the PDF export process that could potentially lead to arbitrary code execution.	7.8	More Details
CVE-2025-11547	AXIS Camera Station Pro contained a flaw to perform a privilege escalation attack on the server as a non-admin user.	7.8	More Details
CVE-2025-15310	Tanium addressed a local privilege escalation vulnerability in Patch Endpoint Tools.	7.8	More Details
CVE-2026-25931	vscode-spell-checker is a basic spell checker that works well with code and documents. Prior to v4.5.4, DocumentSettings._determineIsTrusted treats the configuration value cSpell.trustedWorkspace as the authoritative trust flag. The value defaults to true (package.json) and is read from workspace configuration each time settings are fetched. The code coerces any truthy value to true and forwards it to ConfigLoader.setIsTrusted , which in turn allows JavaScript/TypeScript configuration files (.cspell.config.js/.mjs/.ts , etc.) to be located and executed. Because no VS Code workspace-trust state is consulted, an untrusted workspace can keep the flag true and place a malicious .cspell.config.js ; opening	7.8	More Details

	the workspace causes the extension host to execute attacker-controlled Node.js code with the user’s privileges. This vulnerability is fixed in v4.5.4.		
CVE-2025-15319	Tanium addressed a local privilege escalation vulnerability in Patch Endpoint Tools.	7.8	More Details
CVE-2026-25925	PowerDocu contains a Windows GUI executable to perform technical documentations. Prior to 2.4.0, PowerDocu contains a critical security vulnerability in how it parses JSON files within Flow or App packages. The application blindly trusts the $type property in JSON files, allowing an attacker to instantiate arbitrary .NET objects and execute code. This vulnerability is fixed in 2.4.0.	7.8	More Details
CVE-2026-0536	A maliciously crafted GIF file, when parsed through Autodesk 3ds Max, can cause a Stack-Based Buffer Overflow vulnerability. A malicious actor can leverage this vulnerability to execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2019-25288	Wacom WTabletService 6.6.7-3 contains an unquoted service path vulnerability that allows local attackers to execute malicious code with elevated privileges. Attackers can insert an executable file in the service path to run unauthorized code when the service restarts or the system reboots.	7.8	More Details
CVE-2019-25275	BartVPN 1.2.2 contains an unquoted service path vulnerability in the BartVPNService that allows local attackers to potentially execute arbitrary code with elevated system privileges. Attackers can exploit the unquoted binary path by placing malicious executables in specific file system locations to hijack the service's execution context.	7.8	More Details
CVE-2026-21334	Substance3D - Designer versions 15.1.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-0662	A maliciously crafted project directory, when opening a max file in Autodesk 3ds Max, could lead to execution of arbitrary code in the context of the current process due to an Untrusted Search Path being utilized.	7.8	More Details
CVE-2026-25634	iccDEV provides a set of libraries and tools that allow for the interaction, manipulation, and application of ICC color management profiles. Prior to 2.3.1.4, SrcPixel and DestPixel stack buffers overlap in CIccTagMultiProcessElement::Apply() int IccTagMPE.cpp. This vulnerability is fixed in 2.3.1.4.	7.8	More Details
CVE-2026-25731	calibre is an e-book manager. Prior to 9.2.0, a Server-Side Template Injection (SSTI) vulnerability in Calibre's Templite templating engine allows arbitrary code execution when a user converts an ebook using a malicious custom template file via the --template-html or --template-html-index command-line options. This vulnerability is fixed in 9.2.0.	7.8	More Details
CVE-2026-21533	Improper privilege management in Windows Remote Desktop allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-21519	Access of resource using incompatible type ('type confusion') in Desktop Window Manager allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-21514	Reliance on untrusted inputs in a security decision in Microsoft Office Word allows an unauthorized attacker to bypass a security feature locally.	7.8	More Details
CVE-2026-21357	InDesign Desktop versions 21.1, 20.5.1 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-	After Effects versions 25.6 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of	7.8	More Details

21351	this issue requires user interaction in that a victim must open a malicious file.		
CVE-2026-21335	Substance3D - Designer versions 15.1.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-21330	After Effects versions 25.6 and earlier are affected by an Access of Resource Using Incompatible Type ('Type Confusion') vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-21329	After Effects versions 25.6 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-21328	After Effects versions 25.6 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-0537	A maliciously crafted RGB file, when parsed through Autodesk 3ds Max, can force a Memory Corruption vulnerability. A malicious actor can leverage this vulnerability to execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2026-0538	A maliciously crafted GIF file, when parsed through Autodesk 3ds Max, can force an Out-of-Bounds Write vulnerability. A malicious actor can leverage this vulnerability to execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2026-0659	A maliciously crafted USD file, when loaded or imported into Autodesk Arnold or Autodesk 3ds Max, can force an Out-of-Bounds Write vulnerability. A malicious actor can leverage this vulnerability to execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2026-0660	A maliciously crafted GIF file, when parsed through Autodesk 3ds Max, can cause a Stack-Based Buffer Overflow vulnerability. A malicious actor can leverage this vulnerability to execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2019-25266	Wondershare Application Framework Service 2.4.3.231 contains an unquoted service path vulnerability that allows local attackers to potentially execute arbitrary code with elevated privileges. Attackers can exploit the unquoted service path by placing malicious executables in specific directory locations to hijack the service's execution context.	7.8	More Details
CVE-2026-21341	Substance3D - Stager versions 3.1.6 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-21342	Substance3D - Stager versions 3.1.6 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-21353	DNG SDK versions 1.7.1 2410 and earlier are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-21349	Lightroom Desktop versions 15.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-20979	Improper privilege management in Settings prior to SMR Feb-2026 Release 1 allows local attackers to launch arbitrary activity with Settings privilege.	7.8	More Details
CVE-2019-25305	JumpStart 0.6.0.0 contains an unquoted service path vulnerability in the jswpbapi service running with LocalSystem privileges. Attackers can exploit the unquoted path containing spaces to inject and execute malicious code with elevated system permissions.	7.8	More Details

CVE-2019-25304	SecurOS Enterprise 10.2 contains an unquoted service path vulnerability in the SecurosCtrlService that allows local users to potentially execute code with elevated privileges. Attackers can exploit the unquoted path in C:\Program Files (x86)\ISS\SecurOS\ to insert malicious code that would execute with system-level permissions during service startup.	7.8	More Details
CVE-2026-20983	Improper export of android application components in Samsung Dialer prior to SMR Feb-2026 Release 1 allows local attackers to launch arbitrary activity with Samsung Dialer privilege.	7.8	More Details
CVE-2019-25302	Acer Launch Manager 6.1.7600.16385 contains an unquoted service path vulnerability in the DsiWMIService that allows local users to potentially execute code with elevated privileges. Attackers can exploit the unquoted path in C:\Program Files (x86)\Launch Manager\dsiwmis.exe to insert malicious code that would execute with system-level permissions during service startup.	7.8	More Details
CVE-2026-21352	DNG SDK versions 1.7.1 2410 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2019-25292	Alps HID Monitor Service 8.1.0.10 contains an unquoted service path vulnerability that allows local attackers to potentially execute arbitrary code with elevated privileges. Attackers can exploit the unquoted path in C:\Program Files\Apoint2K\HidMonitorSvc.exe to inject malicious executables and gain system-level access.	7.8	More Details
CVE-2026-21347	Bridge versions 15.1.3, 16.0.1 and earlier are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-21346	Bridge versions 15.1.3, 16.0.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-21345	Substance3D - Stager versions 3.1.6 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-21344	Substance3D - Stager versions 3.1.6 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-21343	Substance3D - Stager versions 3.1.6 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2019-25293	BlueStacks App Player 2.4.44.62.57 contains an unquoted service path vulnerability in the BstHdLogRotatorSvc service that allows local attackers to potentially execute arbitrary code. Attackers can exploit the unquoted path in C:\Program Files (x86)\Bluestacks\HD-LogRotatorService.exe to inject malicious executables and escalate privileges.	7.8	More Details
CVE-2026-0661	A maliciously crafted RGB file, when parsed through Autodesk 3ds Max, can force a Memory Corruption vulnerability. A malicious actor can leverage this vulnerability to execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2019-25272	TexasSoft CyberPlanet 6.4.131 contains an unquoted service path vulnerability in the CCSrvProxy service that allows local attackers to execute arbitrary code. Attackers can exploit the unquoted path in 'C:\Program Files (x86)\TenaxSoft\CyberPlanet\SrvProxy.exe' to	7.8	More Details

	inject malicious executables and gain elevated system privileges.		
CVE-2026-21327	After Effects versions 25.6 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-21239	Heap-based buffer overflow in Windows Kernel allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-21259	Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-21251	Use after free in Windows Cluster Client Failover allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-21326	After Effects versions 25.6 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-21246	Heap-based buffer overflow in Microsoft Graphics Component allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-21245	Heap-based buffer overflow in Windows Kernel allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-21240	Time-of-check time-of-use (toctou) race condition in Windows HTTP.sys allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-21238	Improper access control in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-21318	After Effects versions 25.6 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-21236	Heap-based buffer overflow in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-21232	Untrusted pointer dereference in Windows HTTP.sys allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-21231	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Kernel allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2019-25273	Easy-Hide-IP 5.0.0.3 contains an unquoted service path vulnerability in the EasyRedirect service that allows local attackers to potentially execute arbitrary code. Attackers can exploit the unquoted path in 'C:\Program Files\Easy-Hide-IP\rdr\EasyRedirect.exe' to inject malicious executables and escalate privileges.	7.8	More Details
CVE-2025-15311	Tanium addressed an unauthorized code execution vulnerability in Tanium Appliance.	7.8	More Details
CVE-	MacroHub developed by GIGABYTE has a Local Privilege Escalation vulnerability. Due to the		More

2026-0870	MacroHub application launching external applications with improper privileges, allowing authenticated local attackers to execute arbitrary code with SYSTEM privileges.	7.8	More Details
CVE-2026-21312	Audition versions 25.3 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-21250	Untrusted pointer dereference in Windows HTTP.sys allows an authorized attacker to elevate privileges locally.	7.8	More Details
CVE-2026-21320	After Effects versions 25.6 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-21321	After Effects versions 25.6 and earlier are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-21322	After Effects versions 25.6 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-21323	After Effects versions 25.6 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-21324	After Effects versions 25.6 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2026-21325	After Effects versions 25.6 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2025-13523	Mattermost Confluence plugin version <1.7.0 fails to properly escape user-controlled display names in HTML template rendering which allows authenticated Confluence users with malicious display names to execute arbitrary JavaScript in victim browsers via sending a specially crafted OAuth2 connection link that, when visited, renders the attacker's display name without proper sanitization. Mattermost Advisory ID: MMSA-2025-00557	7.7	More Details
CVE-2026-25506	MUNGE is an authentication service for creating and validating user credentials. From 0.5 to 0.5.17, local attacker can exploit a buffer overflow vulnerability in munged (the MUNGE authentication daemon) to leak cryptographic key material from process memory. With the leaked key material, the attacker could forge arbitrary MUNGE credentials to impersonate any user (including root) to services that rely on MUNGE for authentication. The vulnerability allows a buffer overflow by sending a crafted message with an oversized address length field, corrupting munged's internal state and enabling extraction of the MAC subkey used for credential verification. This vulnerability is fixed in 0.5.18.	7.7	More Details
CVE-2026-25958	Cube is a semantic layer for building data applications. From 0.27.19 to before 1.5.13, 1.4.2, and 1.0.14, it is possible to make a specially crafted request with a valid API token that leads to privilege escalation. This vulnerability is fixed in 1.5.13, 1.4.2, and 1.0.14.	7.7	More Details
	OpenClaw is a personal AI assistant. Prior to version 2026.1.29, there is an OS command injection vulnerability via the Project Root Path in sshNodeCommand. The sshNodeCommand function constructed a shell script without properly escaping the user-supplied project path in an error message. When the cd command failed, the unescaped		

CVE-2026-25157	supplied project path in an error message. When the cd command failed, the unescaped path was interpolated directly into an echo statement, allowing arbitrary command execution on the remote SSH host. The parseSSHTarget function did not validate that SSH target strings could not begin with a dash. An attacker-supplied target like -oProxyCommand=... would be interpreted as an SSH configuration flag rather than a hostname, allowing arbitrary command execution on the local machine. This issue has been patched in version 2026.1.29.	7.7	More Details
CVE-2025-61917	n8n is an open source workflow automation platform. From version 1.65.0 to before 1.114.3, the use of Buffer.allocUnsafe() and Buffer.allocUnsafeSlow() in the task runner allowed untrusted code to allocate uninitialized memory. Such uninitialized buffers could contain residual data from within the same Node.js process (for example, data from prior requests, tasks, secrets, or tokens), resulting in potential information disclosure. This issue has been patched in version 1.114.3.	7.7	More Details
CVE-2026-23689	Due to an uncontrolled resource consumption (Denial of Service) vulnerability, an authenticated attacker with regular user privileges and network access can repeatedly invoke a remote-enabled function module with an excessively large loop-control parameter. This triggers prolonged loop execution that consumes excessive system resources, potentially rendering the system unavailable. Successful exploitation results in a denial-of-service condition that impacts availability, while confidentiality and integrity remain unaffected.	7.7	More Details
CVE-2026-24322	SAP Solution Tools Plug-In (ST-PI) contains a function module that does not perform the necessary authorization checks for authenticated users, allowing sensitive information to be disclosed. This vulnerability has a high impact on confidentiality and does not affect integrity or availability.	7.7	More Details
CVE-2025-70963	Gophish <=0.12.1 is vulnerable to Incorrect Access Control. The administrative dashboard exposes each user’s long-lived API key directly inside the rendered HTML/JavaScript of the page on every login. This makes permanent API credentials accessible to any script running in the browser context.	7.6	More Details
CVE-2025-40587	A vulnerability has been identified in Polarion V2404 (All versions < V2404.5), Polarion V2410 (All versions < V2410.2). The affected application allows arbitrary JavaScript code be included in document titles. This could allow an authenticated remote attacker to conduct a stored cross-site scripting attack by creating specially crafted document titles that are later viewed by other users of the application.	7.6	More Details
CVE-2020-37135	AMSS++ 4.7 contains an authentication bypass vulnerability that allows attackers to access administrative accounts using hardcoded credentials. Attackers can log in with the default admin username and password '1234' to gain unauthorized administrative access to the system.	7.5	More Details
CVE-2020-37143	ProficySCADA for iOS 5.0.25920 contains a denial of service vulnerability that allows attackers to crash the application by manipulating the password input field. Attackers can overwrite the password field with 257 bytes of repeated characters to trigger an application crash and prevent successful authentication.	7.5	More Details
CVE-2026-24491	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.22.0, video_timer can send client notifications after the control channel is closed, dereferencing a freed callback and triggering a use after free. This vulnerability is fixed in 3.22.0.	7.5	More Details
CVE-2020-37150	Edimax EW-7438RPn-v3 Mini 1.27 allows unauthenticated attackers to access the /wizard_reboot.asp page in unsetup mode, which discloses the Wi-Fi SSID and security key. Attackers can retrieve the wireless password by sending a GET request to this endpoint, exposing sensitive information without authentication.	7.5	More Details
CVE-2026-23948	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.22.0, a NULL pointer dereference vulnerability in rdp_write_logon_info_v2() allows a malicious RDP server to crash FreeRDP proxy by sending a specially crafted LogonInfoV2 PDU with cbDomain=0 or cbUserName=0. This vulnerability is fixed in 3.22.0.	7.5	More Details
CVE-	ZOC Terminal 7.25.5 contains a denial of service vulnerability in the private key file input		

2020-37136	field that allows attackers to crash the application. Attackers can overwrite the private key file input with a 2000-byte buffer, causing the application to become unresponsive when attempting to create SSH key files.	7.5	More Details
CVE-2020-37134	UltraVNC Viewer 1.2.4.0 contains a denial of service vulnerability that allows attackers to crash the application by manipulating VNC Server input. Attackers can generate a malformed 256-byte payload and paste it into the VNC Server connection dialog to trigger an application crash.	7.5	More Details
CVE-2020-37133	UltraVNC Launcher 1.2.4.0 contains a denial of service vulnerability in the Repeater Host configuration field that allows attackers to crash the application. Attackers can paste an overly long string of 300 characters into the Repeater Host property to trigger an application crash.	7.5	More Details
CVE-2020-37157	DBPower C300 HD Camera contains a configuration disclosure vulnerability that allows unauthenticated attackers to retrieve sensitive credentials through an unprotected configuration backup endpoint. Attackers can download the configuration file and extract hardcoded username and password by accessing the /tmpfs/config_backup.bin resource.	7.5	More Details
CVE-2026-25724	Claude Code is an agentic coding tool. Prior to version 2.1.7, Claude Code failed to strictly enforce deny rules configured in settings.json when accessing files through symbolic links. If a user explicitly denied Claude Code access to a file (such as /etc/passwd) and Claude Code had access to a symbolic link pointing to that file, it was possible for Claude Code to read the restricted file through the symlink without triggering deny rule enforcement. This issue has been patched in version 2.1.7.	7.5	More Details
CVE-2026-24680	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.22.0, sdl_Pointer_New frees data on failure, then pointer_free calls sdl_Pointer_Free and frees it again, triggering ASan UAF. This vulnerability is fixed in 3.22.0.	7.5	More Details
CVE-2020-37146	ACE Security WiP-90113 HD Camera contains a configuration disclosure vulnerability that allows unauthenticated attackers to retrieve sensitive configuration files. Attackers can access the camera's configuration backup by sending a GET request to the /config_backup.bin endpoint, exposing credentials and system settings.	7.5	More Details
CVE-2026-24675	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.22.0, urb_select_interface can free the device's MS config on error but later code still dereferences it, leading to a use after free in libusb_udev_select_interface. This vulnerability is fixed in 3.22.0.	7.5	More Details
CVE-2026-24682	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.22.0, audin_server_recv_formats frees an incorrect number of audio formats on parse failure (i + i), leading to out-of-bounds access in audio_formats_free. This vulnerability is fixed in 3.22.0.	7.5	More Details
CVE-2026-24678	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.22.0, A capture thread sends sample responses using a freed channel callback after a device channel close, leading to a use after free in ecam_channel_write. This vulnerability is fixed in 3.22.0.	7.5	More Details
CVE-2020-37155	Core FTP Lite 1.3 contains a buffer overflow vulnerability in the username input field that allows attackers to crash the application by supplying oversized input. Attackers can generate a 7000-byte payload of repeated 'A' characters to trigger an application crash without requiring additional interaction.	7.5	More Details
CVE-2026-24683	FreeRDP is a free implementation of the Remote Desktop Protocol. ainput_send_input_event caches channel_callback in a local variable and later uses it without synchronization; a concurrent channel close can free or reinitialize the callback, leading to a use after free. Prior to 3.22.0, This vulnerability is fixed in 3.22.0.	7.5	More Details
CVE-2026-24684	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.22.0, the RDPSND async playback thread can process queued PDUs after the channel is closed and internal state is freed, leading to a use after free in rdpsnd_treat_wave. This vulnerability is fixed in 3.22.0.	7.5	More Details

CVE-2020-37122	SpotFTP-FTP Password Recover 2.4.8 contains a denial of service vulnerability that allows attackers to crash the application by generating a large buffer overflow. Attackers can create a text file with 1000 'Z' characters and input it as a registration code to trigger the application crash.	7.5	More Details
CVE-2026-24676	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.22.0, AUDIN format renegotiation frees the active format list while the capture thread continues using audin->format, leading to a use after free in audio_format_compatible. This vulnerability is fixed in 3.22.0.	7.5	More Details
CVE-2026-2236	C&Cm@il developed by HGiga has a SQL Injection vulnerability, allowing unauthenticated remote attackers to inject arbitrary SQL commands to read database contents.	7.5	More Details
CVE-2026-24681	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.22.0, aAsynchronous bulk transfer completions can use a freed channel callback after URBDRC channel close, leading to a use after free in urb_write_completion. This vulnerability is fixed in 3.22.0.	7.5	More Details
CVE-2020-37109	aSc TimeTables 2020.11.4 contains a denial of service vulnerability that allows attackers to crash the application by overwriting the Subject title field with a large buffer. Attackers can generate a 1000-character buffer and paste it into the Subject title to trigger an application crash and potential instability.	7.5	More Details
CVE-2020-37130	Nsauditor 3.2.0.0 contains a denial of service vulnerability in the registration name input field that allows attackers to crash the application. Attackers can create a malicious payload of 1000 bytes of repeated characters to trigger an application crash when pasted into the registration name field.	7.5	More Details
CVE-2026-25732	NiceGUI is a Python-based UI framework. Prior to 3.7.0, NiceGUI's FileUpload.name property exposes client-supplied filename metadata without sanitization, enabling path traversal when developers use the pattern UPLOAD_DIR / file.name. Malicious filenames containing ../ sequences allow attackers to write files outside intended directories, with potential for remote code execution through application file overwrites in vulnerable deployment patterns. This design creates a prevalent security footgun affecting applications following common community patterns. Note: Exploitation requires application code incorporating file.name into filesystem paths without sanitization. Applications using fixed paths, generated filenames, or explicit sanitization are not affected. This vulnerability is fixed in 3.7.0.	7.5	More Details
CVE-2026-25564	WeKan versions prior to 8.19 contain an insecure direct object reference (IDOR) in checklist creation and related checklist routes. The implementation does not verify that the supplied cardId belongs to the supplied boardId, allowing cross-board ID tampering by manipulating identifiers.	7.5	More Details
CVE-2026-25563	WeKan versions prior to 8.19 contain an insecure direct object reference (IDOR) in checklist creation and related checklist routes. The implementation does not verify that the supplied cardId belongs to the supplied boardId, allowing cross-board ID tampering by manipulating identifiers.	7.5	More Details
CVE-2026-25231	FileRise is a self-hosted web file manager / WebDAV server. Versions prior to 3.3.0, the application contains an unauthenticated file read vulnerability due to the lack of access control on the /uploads directory. Files uploaded to this directory can be accessed directly by any user who knows or can guess the file path, without requiring authentication. As a result, sensitive data could be exposed, and privacy may be breached. This vulnerability is fixed in 3.3.0.	7.5	More Details
CVE-2026-25561	WeKan versions prior to 8.19 contain an authorization weakness in the attachment upload API. The API does not fully validate that provided identifiers (such as boardId, cardId, swimlaneId, and listId) are consistent and refer to a coherent card/board relationship, enabling attempts to upload attachments with mismatched object relationships.	7.5	More Details
CVE-2026-	An unauthenticated remote attacker can bypass authentication by exploiting insufficient URI validation and using path traversal sequences (e.g., /js/../cgi-bin/post.cgi), gaining	7.5	More Details

22905	unauthorized access to protected CGI endpoints and configuration downloads.		More Details
CVE-2026-25762	AdonisJS is a TypeScript-first web framework. Prior to versions 10.1.3 and 11.0.0-next.9, a denial of service (DoS) vulnerability exists in the multipart file handling logic of @adonisjs/bodyparser. When processing file uploads, the multipart parser may accumulate an unbounded amount of data in memory while attempting to detect file types, potentially leading to excessive memory consumption and process termination. This issue has been patched in versions 10.1.3 and 11.0.0-next.9.	7.5	More Details
CVE-2026-25751	FUXA is a web-based Process Visualization (SCADA/HMI/Dashboard) software. An information disclosure vulnerability in FUXA allows an unauthenticated, remote attacker to retrieve sensitive administrative database credentials. Exploitation allows an unauthenticated, remote attacker to obtain the full system configuration, including administrative credentials for the InfluxDB database. Possession of these credentials may allow an attacker to authenticate directly to the database service, enabling them to read, modify, or delete all historical process data, or perform a Denial of Service by corrupting the database. This affects FUXA through version 1.2.9. This issue has been patched in FUXA version 1.2.10.	7.5	More Details
CVE-2026-25121	apko allows users to build and publish OCI container images built from apk packages. From version 0.14.8 to before 1.1.1, a path traversal vulnerability was discovered in apko's dirFS filesystem abstraction. An attacker who can supply a malicious APK package (e.g., via a compromised or typosquatted repository) could create directories or symlinks outside the intended installation root. The MkdirAll, Mkdir, and Symlink methods in pkg/apk/fs/rwosfs.go use filepath.Join() without validating that the resulting path stays within the base directory. This issue has been patched in version 1.1.1.	7.5	More Details
CVE-2020-37107	Core FTP LE 2.2 contains a denial of service vulnerability that allows attackers to crash the application by overwriting the account field with a large buffer. Attackers can create a text file with 20,000 repeated characters and paste it into the account field to cause the application to become unresponsive and require reinstallation.	7.5	More Details
CVE-2026-25644	DataHub is an open-source metadata platform. Prior to version 1.3.1.8, the LDAP ingestion source is vulnerable to MITM attack through TLS downgrade. This issue has been patched in version 1.3.1.8.	7.5	More Details
CVE-2026-2093	Docpedia developed by Flowring has a SQL Injection vulnerability, allowing unauthenticated remote attackers to inject arbitrary SQL commands to read database contents.	7.5	More Details
CVE-2026-25992	SiYuan is a personal knowledge management system. Prior to 3.5.5, the /api/file/getFile endpoint uses case-sensitive string equality checks to block access to sensitive files. On case-insensitive file systems such as Windows, attackers can bypass restrictions using mixed-case paths and read protected configuration files. This vulnerability is fixed in 3.5.5.	7.5	More Details
CVE-2026-25611	A series of specifically crafted, unauthenticated messages can exhaust available memory and crash a MongoDB server.	7.5	More Details
CVE-2026-23897	Apollo Server is an open-source, spec-compliant GraphQL server that's compatible with any GraphQL client, including Apollo Client. In versions from 2.0.0 to 3.13.0, 4.2.0 to before 4.13.0, and 5.0.0 to before 5.4.0, the default configuration of startStandaloneServer from @apollo/server/standalone is vulnerable to denial of service (DoS) attacks through specially crafted request bodies with exotic character set encodings. This issue does not affect users that use @apollo/server as a dependency for integration packages, like @as-integrations/express5 or @as-integrations/next, only direct usage of startStandaloneServer.	7.5	More Details
CVE-2026-25577	Emmett is a framework designed to simplify your development process. Prior to 1.3.11, the cookies property in mmett_core.http.wrappers.Request does not handle CookieError exceptions when parsing malformed Cookie headers. This allows unauthenticated attackers to trigger HTTP 500 errors and cause denial of service. This vulnerability is fixed in 1.3.11.	7.5	More Details
CVE-	apko allows users to build and publish OCI container images built from apk packages. From version 0.14.8 to before 1.1.1, an attacker who controls or compromises an APK repository used by apko could cause resource exhaustion on the build host. The ExpandApk function in		More

2026-25140	pkg/apk/expandapk/expandapk.go expands .apk streams without enforcing decompression limits, allowing a malicious repository to serve a small, highly-compressed .apk that inflates into a large tar stream, consuming excessive disk space and CPU time, causing build failures or denial of service. This issue has been patched in version 1.1.1.	7.5	More Details
CVE-2026-24735	Exposure of Private Personal Information to an Unauthorized Actor vulnerability in Apache Answer. This issue affects Apache Answer: through 1.7.1. An unauthenticated API endpoint incorrectly exposes full revision history for deleted content. This allows unauthorized user to retrieve restricted or sensitive information. Users are recommended to upgrade to version 2.0.0, which fixes the issue.	7.5	More Details
CVE-2026-0490	SAP BusinessObjects BI Platform allows an unauthenticated attacker to craft a specific network request to the trusted endpoint that breaks the authentication, which prevents the legitimate users from accessing the platform. As a result, it has a high impact on the availability but no impact on the confidentiality and integrity.	7.5	More Details
CVE-2026-2268	The Ninja Forms plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.14.0. This is due to the unsafe application of the `ninja_forms_merge_tags` filter to user-supplied input within repeater fields, which allows the resolution of `{post_meta:KEY}` merge tags without authorization checks. This makes it possible for unauthenticated attackers to extract arbitrary post metadata from any post on the site, including sensitive data such as WooCommerce billing emails, API keys, private tokens, and customer personal information via the `nf_ajax_submit` AJAX action.	7.5	More Details
CVE-2026-21511	Deserialization of untrusted data in Microsoft Office Outlook allows an unauthorized attacker to perform spoofing over a network.	7.5	More Details
CVE-2026-20119	A vulnerability in the text rendering subsystem of Cisco TelePresence Collaboration Endpoint (CE) Software and Cisco RoomOS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of input received by an affected device. An attacker could exploit this vulnerability by getting the affected device to render crafted text, for example, a crafted meeting invitation. As indicated in the CVSS score, no user interaction is required, such as accepting the meeting invitation. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.	7.5	More Details
CVE-2026-21260	Exposure of sensitive information to an unauthorized actor in Microsoft Office Outlook allows an unauthorized attacker to perform spoofing over a network.	7.5	More Details
CVE-2025-22453	Improper input validation for some Server Firmware Update Utility(SysFwUpdt) before version 16.0.12 within Ring 3: User Applications may allow an escalation of privilege. System software adversary with a privileged user combined with a high complexity attack may enable local code execution. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	7.5	More Details
CVE-2026-21243	Null pointer dereference in Windows LDAP - Lightweight Directory Access Protocol allows an unauthorized attacker to deny service over a network.	7.5	More Details
CVE-2026-21218	Improper handling of missing special element in .NET allows an unauthorized attacker to perform spoofing over a network.	7.5	More Details
CVE-2026-20846	Buffer over-read in Windows GDI+ allows an unauthorized attacker to deny service over a network.	7.5	More Details
CVE-	Connections received from the proxy port may not count towards total accepted		

CVE-2026-1848	connections, resulting in server crashes if the total number of connections exceeds available resources. This only applies to connections accepted from the proxy port, pending the proxy protocol header.	7.5	More Details
CVE-2025-71031	Water-Melon Melon commit 9df9292 and below is vulnerable to Denial of Service. The HTTP component doesn't have any maximum length. As a result, an excessive request header could cause a denial of service by consuming RAM memory.	7.5	More Details
CVE-2026-25808	Hollo is a federated single-user microblogging software designed to be federated through ActivityPub. Prior to 0.6.20 and 0.7.2, there is a security vulnerability where DMs and followers-only posts were exposed through the ActivityPub outbox endpoint without authorization. This vulnerability is fixed in 0.6.20 and 0.7.2.	7.5	More Details
CVE-2026-1507	The affected products are vulnerable to an uncaught exception that could allow an unauthenticated attacker to remotely crash core PI services resulting in a denial-of-service.	7.5	More Details
CVE-2026-0485	SAP BusinessObjects BI Platform allows an unauthenticated attacker to send specially crafted requests that could cause the Content Management Server (CMS) to crash and automatically restart. By repeatedly submitting these requests, the attacker could induce a persistent service disruption, rendering the CMS completely unavailable. Successful exploitation results in a high impact on availability, while confidentiality and integrity remain unaffected.	7.5	More Details
CVE-2026-25892	Adminer is open-source database management software. Adminer v5.4.1 and earlier has a version check mechanism where adminer.org sends signed version info via JavaScript postMessage, which the browser then POSTs to ?script=version. This endpoint lacks origin validation and accepts POST data from any source. An attacker can POST version[] parameter which PHP converts to an array. On next page load, openssl_verify() receives this array instead of string and throws TypeError, returning HTTP 500 to all users. Upgrade to Adminer 5.4.2.	7.5	More Details
CVE-2026-25961	SumatraPDF is a multi-format reader for Windows. In 3.5.0 through 3.5.2, SumatraPDF's update mechanism disables TLS hostname verification (INTERNET_FLAG_IGNORE_CERT_CN_INVALID) and executes installers without signature checks. A network attacker with any valid TLS certificate (e.g., Let's Encrypt) can intercept the update check request, inject a malicious installer URL, and achieve arbitrary code execution.	7.5	More Details
CVE-2026-25639	Axios is a promise based HTTP client for the browser and Node.js. Prior to 1.13.5, the mergeConfig function in axios crashes with a TypeError when processing configuration objects containing __proto__ as an own property. An attacker can trigger this by providing a malicious configuration object created via JSON.parse(), causing complete denial of service. This vulnerability is fixed in 1.13.5.	7.5	More Details
CVE-2025-15285	The SEO Flow by LupsOnline plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the checkBlogAuthentication() and checkCategoryAuthentication() functions in all versions up to, and including, 2.2.1. These authorization functions only implement basic API key authentication but fail to implement WordPress capability checks. This makes it possible for unauthenticated attackers to create, modify, and delete blog posts and categories.	7.5	More Details
CVE-2025-15268	The Infility Global plugin for WordPress is vulnerable to unauthenticated SQL Injection via the 'infility_get_data' API action in all versions up to, and including, 2.14.46. 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 - with certain server configurations - additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details
CVE-2026-25791	Sliver is a command and control framework that uses a custom Wireguard netstack. Prior to 1.7.0, the DNS C2 listener accepts unauthenticated TOTP bootstrap messages and allocates server-side DNS sessions without validating OTP values, even when EnforceOTP is enabled. Because sessions are stored without a cleanup/expiry path in this flow, an unauthenticated	7.5	More Details

	remote actor can repeatedly create sessions and drive memory exhaustion. This vulnerability is fixed in 1.7.0.		
CVE-2026-25478	Litestar is an Asynchronous Server Gateway Interface (ASGI) framework. Prior to 2.20.0, CORSConfig.allowed_origins_regex is constructed using a regex built from configured allowlist values and used with fullmatch() for validation. Because metacharacters are not escaped, a malicious origin can match unexpectedly. The check relies on allowed_origins_regex.fullmatch(origin). This vulnerability is fixed in 2.20.0.	7.4	More Details
CVE-2025-68621	Trilium Notes is an open-source, cross-platform hierarchical note taking application with focus on building large personal knowledge bases. Prior to 0.101.0, a critical timing attack vulnerability in Trilium's sync authentication endpoint allows unauthenticated remote attackers to recover HMAC authentication hashes byte-by-byte through statistical timing analysis. This enables complete authentication bypass without password knowledge, granting full read/write access to victim's knowledge base. This vulnerability is fixed in 0.101.0.	7.4	More Details
CVE-2026-1707	pgAdmin versions 9.11 are affected by a Restore restriction bypass via key disclosure vulnerability that occurs when running in server mode and performing restores from PLAIN-format dump files. An attacker with access to the pgAdmin web interface can observe an active restore operation, extract the `\restrict` key in real time, and race the restore process by overwriting the restore script with a payload that re-enables meta-commands using `\unrestrict <key>`. This results in reliable command execution on the pgAdmin host during the restore operation.	7.4	More Details
CVE-2026-2172	A vulnerability was determined in code-projects Online Application System for Admission 1.0. Affected by this vulnerability is an unknown functionality of the file enrollment/index.php of the component Login Endpoint. Executing a manipulation can lead to sql injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2026-2164	A security flaw has been discovered in detronetdip E-commerce 1.0.0. This issue affects some unknown processing of the file /seller/assets/backend/profile/addadhar.php. Performing a manipulation of the argument File results in unrestricted upload. 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.	7.3	More Details
CVE-2026-2197	A vulnerability was determined in code-projects Online Reviewer System 1.0. Impacted is an unknown function of the file /system/system/admins/assessments/pretest/exam-delete.php. This manipulation of the argument test_id 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-2026-2165	A weakness has been identified in detronetdip E-commerce 1.0.0. Impacted is an unknown function of the file /Admin/assets/backend/seller/add_seller.php of the component Account Creation Endpoint. Executing a manipulation of the argument email can lead to missing authentication. The attack can be executed 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-2026-2166	A security vulnerability has been detected in code-projects Online Reviewer System 1.0. The affected element is an unknown function of the file /login/index.php of the component Login. The manipulation of the argument username/password leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2026-2083	A security flaw has been discovered in code-projects Social Networking Site 1.0. This affects an unknown function of the file /delete_post.php. Performing a manipulation of the argument ID 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.	7.3	More Details
CVE-2026-	A vulnerability was found in code-projects Online Reviewer System 1.0. This issue affects some unknown processing of the file /system/system/admins/assessments/pretest/exam-update.php. The manipulation of the argument test_id results in sql injection. The attack	7.3	More Details

2196	update.php. The manipulation of the argument test_id results in sql injection. The attack may be performed from remote. The exploit has been made public and could be used.		Details
CVE-2026-2171	A vulnerability was found in code-projects Online Student Management System 1.0. Affected is an unknown function of the file accounts.php of the component Login. Performing a manipulation of the argument username/password results in sql injection. The attack can be initiated remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2026-2060	A vulnerability was found in code-projects Simple Blood Donor Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /simpleblooddonor/editcampaignform.php. Performing a manipulation of the argument ID results in sql injection. It is possible to initiate the attack remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2026-2189	A vulnerability was identified in itsourcecode School Management System 1.0. This affects an unknown function of the file /ramonsys/report/index.php. The manipulation of the argument ay leads to sql injection. The attack can be initiated remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2026-21235	Use after free in Microsoft Graphics Component allows an authorized attacker to elevate privileges locally.	7.3	More Details
CVE-2026-2173	A vulnerability was identified in code-projects Online Examination System 1.0. Affected by this issue is some unknown functionality of the file login.php. The manipulation of the argument username/password leads to sql injection. The attack may be initiated remotely.	7.3	More Details
CVE-2026-2174	A security flaw has been discovered in code-projects Contact Management System 1.0. This affects an unknown part of the component CRUD Endpoint. The manipulation of the argument ID results in improper authentication. The attack may be launched remotely.	7.3	More Details
CVE-2026-21248	Heap-based buffer overflow in Windows Hyper-V allows an authorized attacker to execute code locally.	7.3	More Details
CVE-2026-2195	A vulnerability has been found in code-projects Online Reviewer System 1.0. This vulnerability affects unknown code of the file /system/system/admins/assessments/pretest/questions-view.php. The manipulation of the argument ID leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2026-2161	A vulnerability was found in itsourcecode Directory Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/forget-password.php. The manipulation of the argument email results in sql injection. The attack can be launched remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2026-2177	A vulnerability has been found in SourceCodester Prison Management System 1.0. The impacted element is an unknown function of the component Login. The manipulation leads to session fixiation. 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-2026-2190	A security flaw has been discovered in itsourcecode School Management System 1.0. This impacts an unknown function of the file /ramonsys/user/controller.php. The manipulation of the argument ID results in sql injection. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks.	7.3	More Details
CVE-2026-2184	A vulnerability was detected in Great Developers Certificate Generation System up to 97171bb0e5e22e52eacf4e4fa81773e5f3cffb73. This vulnerability affects unknown code of the file /restructured/csv.php. The manipulation of the argument photo results in os command injection. The attack can be executed remotely. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable. The code repository of the project has not been active for many years.	7.3	More Details
CVE-			

2026-21244	Heap-based buffer overflow in Windows Hyper-V allows an authorized attacker to execute code locally.	7.3	More Details
CVE-2026-2113	A security vulnerability has been detected in yuan1994 tpadmin up to 1.3.12. This affects an unknown part in the library /public/static/admin/lib/webuploader/0.1.5/server/preview.php of the component WebUploader. The manipulation leads to deserialization. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	7.3	More Details
CVE-2026-2158	A vulnerability was detected in code-projects Student Web Portal 1.0. This impacts an unknown function of the file /check_user.php. Performing a manipulation of the argument Username results in sql injection. It is possible to initiate the attack remotely.	7.3	More Details
CVE-2026-2090	A vulnerability was determined in SourceCodester Online Class Record System 1.0. This issue affects some unknown processing of the file /admin/message/search.php. Executing a manipulation of the argument term can lead to sql injection. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2026-2018	A flaw has been found in itsourcecode School Management System 1.0. This affects an unknown part of the file /ramonsys/settings/controller.php. This manipulation of the argument ID causes sql injection. It is possible to initiate the attack remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2026-2057	A vulnerability was detected in SourceCodester Medical Center Portal Management System 1.0. This affects an unknown function of the file /login.php. The manipulation of the argument User results in sql injection. The attack can be executed remotely. The exploit is now public and may be used.	7.3	More Details
CVE-2026-2114	A vulnerability was detected in itsourcecode Society Management System 1.0. This vulnerability affects unknown code of the file /admin/edit_admin.php. The manipulation of the argument admin_id results in sql injection. The attack may be performed from remote. The exploit is now public and may be used.	7.3	More Details
CVE-2026-2014	A security flaw has been discovered in itsourcecode Student Management System 1.0. This impacts an unknown function of the file /ramonsys/billing/index.php. Performing a manipulation of the argument ID results in sql injection. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks.	7.3	More Details
CVE-2026-2013	A vulnerability was identified in itsourcecode Student Management System 1.0. This affects an unknown function of the file /ramonsys/soa/index.php. Such manipulation of the argument ID leads to sql injection. The attack may be launched remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2026-2115	A flaw has been found in itsourcecode Society Management System 1.0. This issue affects some unknown processing of the file /admin/delete_expenses.php. This manipulation of the argument expenses_id causes sql injection. It is possible to initiate the attack remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2026-2116	A vulnerability has been found in itsourcecode Society Management System 1.0. Impacted is an unknown function of the file /admin/edit_expenses.php. Such manipulation of the argument expenses_id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2026-2117	A vulnerability was found in itsourcecode Society Management System 1.0. The affected element is an unknown function of the file /admin/edit_activity.php. Performing a manipulation of the argument activity_id results in sql injection. The attack can be initiated remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2026-2012	A vulnerability was determined in itsourcecode Student Management System 1.0. The impacted element is an unknown function of the file /ramonsys/facultyloading/index.php. This manipulation of the argument ID causes sql injection. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details

CVE-2026-2011	A vulnerability was found in itsourcecode Student Management System 1.0. The affected element is an unknown function of the file /ramonsys/enrollment/controller.php. The manipulation of the argument ID results in sql injection. The attack can be launched remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2026-24925	Heap-based buffer overflow vulnerability in the image module. Impact: Successful exploitation of this vulnerability may affect availability.	7.3	More Details
CVE-2026-2087	A flaw has been found in SourceCodester Online Class Record System 1.0. Affected by this issue is some unknown functionality of the file /admin/login.php. This manipulation of the argument user_email causes sql injection. The attack may be initiated remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2026-2089	A vulnerability was found in SourceCodester Online Class Record System 1.0. This vulnerability affects unknown code of the file /admin/subject/controller.php. Performing a manipulation of the argument ID results in sql injection. Remote exploitation of the attack is possible. The exploit has been made public and could be used.	7.3	More Details
CVE-2026-2199	A security flaw has been discovered in code-projects Online Reviewer System 1.0. The impacted element is an unknown function of the file /reviewer/system/system/admins/manage/users/user-delete.php. Performing a manipulation of the argument ID 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-2026-2088	A vulnerability has been found in PHPGurukul Beauty Parlour Management System 1.1. This affects an unknown part of the file /admin/accepted-appointment.php. Such manipulation of the argument delid leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2026-2058	A flaw has been found in mathurvishal CloudClassroom-PHP-Project up to 5dadec098bfbbf3300d60c3494db3fb95b66e7be. This impacts an unknown function of the file /postquerypublic.php of the component Post Query Details Page. This manipulation of the argument gnamex causes sql injection. The attack is possible to be carried out remotely. The exploit has been published and may be used. This product adopts a rolling release strategy to maintain continuous delivery. Therefore, version details for affected or updated releases cannot be specified. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-2073	A vulnerability was determined in itsourcecode School Management System 1.0. This affects an unknown function of the file /ramonsys/user/index.php. Executing a manipulation of the argument ID can lead to sql injection. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2026-2059	A vulnerability has been found in SourceCodester Medical Center Portal Management System 1.0. Affected is an unknown function of the file /emp_edit1.php. Such manipulation of the argument ID leads to sql injection. The attack may be performed from remote. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2026-2132	A security flaw has been discovered in code-projects Online Music Site 1.0. This issue affects some unknown processing of the file /Administrator/PHP/AdminUpdateCategory.php. The manipulation of the argument txtcat results in sql injection. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks.	7.3	More Details
CVE-2026-24045	Docmost is open-source collaborative wiki and documentation software. From g and before 0.25.0, the public share page functionality in Docmost does not properly HTML-escape page titles before inserting them into meta tags and the title tag. This allows Stored Cross-Site Scripting (XSS) attacks, where an attacker can execute arbitrary JavaScript in the context of any user who opens a shared page link. This vulnerability is fixed in 0.25.0.	7.3	More Details
CVE-2026-	A weakness has been identified in code-projects Online Music Site 1.0. Impacted is an unknown function of the file /Administrator/PHP/AdminUpdateCategory.php. This manipulation of the argument txtimage causes unrestricted upload. The attack is possible to	7.3	More Details

2133	be carried out remotely. The exploit has been made available to the public and could be used for attacks.		Details
CVE-2026-2136	A flaw has been found in projectworlds Online Food Ordering System 1.0. This affects an unknown function of the file /view-ticket.php. Executing a manipulation of the argument ID can lead to sql injection. It is possible to launch the attack remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2026-2198	A vulnerability was identified in code-projects Online Reviewer System 1.0. The affected element is an unknown function of the file /system/system/admins/assessments/pretest/loaddata.php. Such manipulation of the argument difficulty_id leads to sql injection. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2026-21247	Improper input validation in Windows Hyper-V allows an authorized attacker to execute code locally.	7.3	More Details
CVE-2026-2220	A vulnerability was identified in code-projects Online Reviewer System 1.0. This impacts an unknown function of the file /system/system/admins/assessments/pretest/btn_functions.php. Such manipulation of the argument difficulty_id leads to sql injection. The attack can be executed remotely. The exploit is publicly available and might be used.	7.3	More Details
CVE-2026-2225	A flaw has been found in itsourcecode News Portal Project 1.0. This vulnerability affects unknown code of the file /admin/index.php of the component Administrator Login. This manipulation of the argument email causes sql injection. The attack can be initiated remotely. The exploit has been published and may be used.	7.3	More Details
CVE-2025-10463	Improper Authentication vulnerability in Birtech Information Technologies Industry and Trade Ltd. Co. Senseway allows Authentication Abuse.This issue affects Senseway: through 09022026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-2221	A security flaw has been discovered in code-projects Online Reviewer System 1.0. Affected is an unknown function of the file /login/index.php of the component Login. Performing a manipulation of the argument Username results in sql injection. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks.	7.3	More Details
CVE-2026-2223	A security vulnerability has been detected in code-projects Online Reviewer System 1.0. Affected by this issue is some unknown functionality of the file /system/system/students/assessments/pretest/take/index.php. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used.	7.3	More Details
CVE-2026-0508	The SAP BusinessObjects Business Intelligence Platform allows an authenticated attacker with high privileges to insert malicious URL within the application. Upon successful exploitation, the victim may click on this malicious URL, resulting in an unvalidated redirect to the attacker-controlled domain and subsequently download the malicious content. This vulnerability has a high impact on the confidentiality and integrity of the application, with no effect on the availability of the application.	7.3	More Details
CVE-2026-2211	A vulnerability was determined in code-projects Online Music Site 1.0. Affected is an unknown function of the file /Administrator/PHP/AdminDeleteCategory.php. Executing a manipulation of the argument ID can lead to sql injection. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized.	7.3	More Details
CVE-2026-2212	A vulnerability was identified in code-projects Online Music Site 1.0. Affected by this vulnerability is an unknown functionality of the file /Administrator/PHP/AdminEditCategory.php. The manipulation of the argument ID leads to sql injection. The attack is possible to be carried out remotely. The exploit is publicly available and might be used.	7.3	More Details
	A security flaw has been discovered in Open5GS up to 2.7.6. Affected by this vulnerability is		

CVE-2025-15555	the function hss_ogs_diam_cx_mar_cb of the file src/hss/hss-cx-path.c of the component VoLTE Cx-Test. The manipulation of the argument OGS_KEY_LEN results in stack-based buffer overflow. The attack may be launched remotely. The patch is identified as 54dda041211098730221d0ae20a2f9f9173e7a21. A patch should be applied to remediate this issue.	7.3	More Details
CVE-2026-2217	A vulnerability was found in itsourcecode Event Management System 1.0. The impacted element is an unknown function of the file /admin/manage_user.php. The manipulation of the argument ID results in sql injection. The attack may be launched remotely. The exploit has been made public and could be used.	7.3	More Details
CVE-2026-2120	A vulnerability was identified in D-Link DIR-823X 250416. This affects an unknown function of the file /goform/set_server_settings of the component Configuration Parameter Handler. The manipulation of the argument terminal_addr/server_ip/server_port leads to os command injection. The attack may be initiated remotely. The exploit is publicly available and might be used.	7.2	More Details
CVE-2025-11730	A post-authentication command injection vulnerability in the Dynamic DNS (DDNS) configuration CLI command in Zyxel ATP series firmware versions from V5.35 through V5.41, USG FLEX series firmware versions from V5.35 through V5.41, USG FLEX 50(W) series firmware versions from V5.35 through V5.41, and USG20(W)-VPN series firmware versions from V5.35 through V5.41 could allow an authenticated attacker with administrator privileges to execute operating system (OS) commands on an affected device by supplying a specially crafted string as an argument to the CLI command.	7.2	More Details
CVE-2026-2175	A weakness has been identified in D-Link DIR-823X 250416. This vulnerability affects the function sub_420618 of the file /goform/set_upnp. This manipulation of the argument upnp_enable causes os command injection. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks.	7.2	More Details
CVE-2026-2080	A vulnerability has been found in UTT HiPER 810 1.7.4-141218. This issue affects the function setSysAdm of the file /goform/formUser. The manipulation of the argument passwd1 leads to command injection. Remote exploitation of the attack is possible. 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.	7.2	More Details
CVE-2026-2129	A vulnerability was found in D-Link DIR-823X 250416. Affected by this issue is some unknown functionality of the file /goform/set_ac_status. Performing a manipulation of the argument ac_ipaddr/ac_ipstatus/ap_randtime results in os command injection. The attack may be initiated remotely. The exploit has been made public and could be used.	7.2	More Details
CVE-2026-2151	A vulnerability has been found in D-Link DIR-615 4.10. This affects an unknown part of the file adv_firewall.php of the component DMZ Host Feature. Such manipulation of the argument dmz_ipaddr leads to os command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	7.2	More Details
CVE-2026-2084	A weakness has been identified in D-Link DIR-823X 250416. This impacts an unknown function of the file /goform/set_language. Executing a manipulation of the argument langSelection can lead to os command injection. It is possible to launch the attack remotely. The exploit has been made available to the public and could be used for attacks.	7.2	More Details
CVE-2026-21743	A missing authorization vulnerability in Fortinet FortiAuthenticator 6.6.0 through 6.6.6, FortiAuthenticator 6.5 all versions, FortiAuthenticator 6.4 all versions, FortiAuthenticator 6.3 all versions may allow a read-only user to make modification to local users via a file upload to an unprotected endpoint.	7.2	More Details
CVE-2026-2182	A weakness has been identified in UTT 进取 521G 3.1.1-190816. Affected by this issue is the function doSystem of the file /goform/setSysAdm. Executing a manipulation of the argument passwd1 can lead to command injection. The attack may be launched remotely. The exploit has been made available to the public and could be used for attacks.	7.2	More Details
CVE-	A security flaw has been discovered in D-Link DIR-823X 250416. The affected element is the function sub_4208A0 of the file /goform/set_dmz of the component Configuration Handler.		More

2026-2155	The manipulation of the argument dmz_host/dmz_enable results in os command injection. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks.	7.2	More Details
CVE-2026-2152	A vulnerability was found in D-Link DIR-615 4.10. This vulnerability affects unknown code of the file adv_routing.php of the component Web Configuration Interface. Performing a manipulation of the argument dest_ip/ submask/ gw results in os command injection. The attack may be initiated remotely. The exploit has been made public and could be used. This vulnerability only affects products that are no longer supported by the maintainer.	7.2	More Details
CVE-2026-0845	The WCFM – Frontend Manager for WooCommerce along with Bookings Subscription Listings Compatible plugin for WordPress is vulnerable to unauthorized modification of data that can lead to privilege escalation due to a missing capability check on the 'WCFM_Settings_Controller::processing' function in all versions up to, and including, 6.7.24. This makes it possible for authenticated attackers, with Shop Manager-level access and above, to update arbitrary options on the WordPress site. This can be leveraged to update the default role for registration to administrator and enable user registration for attackers to gain administrative user access to a vulnerable site.	7.2	More Details
CVE-2026-2085	A security vulnerability has been detected in D-Link DWR-M921 1.1.50. Affected is the function sub_419F20 of the file /boafrm/formUSSDSetup of the component USSD Configuration Endpoint. The manipulation of the argument ussdValue leads to command injection. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used.	7.2	More Details
CVE-2026-2143	A security vulnerability has been detected in D-Link DIR-823X 250416. This issue affects some unknown processing of the file /goform/set_ddns of the component DDNS Service. The manipulation of the argument ddnsType/ddnsDomainName/ddnsUserName/ddnsPwd leads to os command injection. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used.	7.2	More Details
CVE-2026-2142	A weakness has been identified in D-Link DIR-823X 250416. This vulnerability affects the function sub_420688 of the file /goform/set_qos. Executing a manipulation can lead to os command injection. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks.	7.2	More Details
CVE-2026-2157	A security vulnerability has been detected in D-Link DIR-823X 250416. This affects the function sub_4175CC of the file /goform/set_static_route_table. Such manipulation of the argument interface/destip/netmask/gateway/metric leads to os command injection. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.	7.2	More Details
CVE-2026-25754	AdonisJS is a TypeScript-first web framework. Prior to versions 10.1.3 and 11.0.0-next.9, a prototype pollution vulnerability in AdonisJS multipart form-data parsing may allow a remote attacker to manipulate object prototypes at runtime. This issue has been patched in versions 10.1.3 and 11.0.0-next.9.	7.2	More Details
CVE-2026-2260	A vulnerability was found in D-Link DCS-931L up to 1.13.0. This affects an unknown part of the file /goform/setSysAdmin. The manipulation of the argument AdminID results in os command injection. The attack can be executed remotely. The exploit has been made public and could be used. This vulnerability only affects products that are no longer supported by the maintainer.	7.2	More Details
CVE-2026-1294	The All In One Image Viewer Block plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 1.0.2 due to missing authorization and URL validation on the image-proxy REST API endpoint. This makes it possible for unauthenticated attackers to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	7.2	More Details
CVE-2026-2118	A vulnerability was determined in UTT HiPER 810 1.7.4-141218. The impacted element is the function sub_4407D4 of the file /goform/formReleaseConnect of the component rehttpd. Executing a manipulation of the argument Isp_Name can lead to command injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be	7.2	More Details

	utilized.		
CVE-2026-2210	A vulnerability has been found in D-Link DIR-823X 250416. This affects the function sub_4211C8 of the file /goform/set_filtering. Such manipulation leads to os command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.2	More Details
CVE-2025-70073	An issue in ChestnutCMS v.1.5.8 and before allows a remote attacker to execute arbitrary code via the template creation function	7.2	More Details
CVE-2026-2192	A security vulnerability has been detected in Tenda AC9 15.03.06.42_multi. Affected by this vulnerability is the function formGetRebootTimer. Such manipulation of the argument sys.schedulereboot.start_time/sys.schedulereboot.end_time leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed publicly and may be used.	7.2	More Details
CVE-2026-2188	A vulnerability was determined in UTT 进取 521G 3.1.1-190816. The impacted element is the function sub_446B18 of the file /goform/formPdbUpConfig. Executing a manipulation of the argument policyNames can lead to os command injection. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized.	7.2	More Details
CVE-2026-1866	The Name Directory plugin for WordPress is vulnerable to Stored Cross-Site Scripting via double HTML-entity encoding in all versions up to, and including, 1.32.0. This is due to the plugin's sanitization function calling `html_entity_decode()` before `wp_kses()`, and then calling `html_entity_decode()` again on output. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page via the 'name_directory_name' and 'name_directory_description' parameters in the public submission form granted they can trick the site administrator into approving their submission or auto-publish is enabled.	7.2	More Details
CVE-2026-23572	Improper access control in the TeamViewer Full and Host clients (Windows, macOS, Linux) prior version 15.74.5 allows an authenticated user to bypass additional access controls with “Allow after confirmation” configuration in a remote session. An exploit could result in unauthorized access prior to local confirmation. The user needs to be authenticated for the remote session via ID/password, Session Link, or Easy Access as a prerequisite to exploit this vulnerability.	7.2	More Details
CVE-2026-2191	A weakness has been identified in Tenda AC9 15.03.06.42_multi. Affected is the function formGetDdosDefenceList. This manipulation of the argument security.ddos.map causes stack-based buffer overflow. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks.	7.2	More Details
CVE-2019-25298	html5_snmp 1.11 contains multiple SQL injection vulnerabilities that allow attackers to manipulate database queries through Router_ID and Router_IP parameters. Attackers can exploit error-based, time-based, and union-based injection techniques to potentially extract or modify database information by sending crafted payloads.	7.1	More Details
CVE-2019-25299	RimbaLinux AhadPOS 1.11 contains a SQL injection vulnerability in the 'alamatCustomer' parameter that allows attackers to manipulate database queries through crafted POST requests. Attackers can exploit time-based and boolean-based blind SQL injection techniques to extract information or potentially interact with the underlying database.	7.1	More Details
CVE-2019-25300	thejshen Globitek CMS 1.4 contains a SQL injection vulnerability that allows attackers to manipulate database queries through the 'id' GET parameter. Attackers can exploit boolean-based, time-based, and UNION-based SQL injection techniques to potentially extract or modify database information.	7.1	More Details
CVE-2019-25303	TheJshen ContentManagementSystem 1.04 contains a SQL injection vulnerability that allows attackers to manipulate database queries through the 'id' GET parameter. Attackers can exploit boolean-based, time-based, and UNION-based SQL injection techniques to extract or manipulate database information by crafting malicious query payloads.	7.1	More Details
	Infor SyteLine ERP uses hard-coded static cryptographic keys to encrypt stored credentials,		

CVE-2026-2103	including user passwords, database connection strings, and API keys. The encryption keys are identical across all installations. An attacker with access to the application binary and database can decrypt all stored credentials.	7.1	More Details
CVE-2026-25640	Pydantic AI is a Python agent framework for building applications and workflows with Generative AI. From 1.34.0 to before 1.51.0, a path traversal vulnerability in the Pydantic AI web UI allows an attacker to serve arbitrary JavaScript in the context of the application by crafting a malicious URL. In affected versions, the CDN URL is constructed using a version query parameter from the request URL. This parameter is not validated, allowing path traversal sequences that cause the server to fetch and serve attacker-controlled HTML/JavaScript from an arbitrary source on the same CDN, instead of the legitimate chat UI package. If a victim clicks the link or visits it via an iframe, attacker-controlled code executes in their browser, enabling theft of chat history and other client-side data. This vulnerability only affects applications that use Agent.to_web to serve a chat interface and clai web to serve a chat interface from the CLI. These are typically run locally (on localhost), but may also be deployed on a remote server. This vulnerability is fixed in 1.51.0.	7.1	More Details
CVE-2025-62676	An Improper Link Resolution Before File Access ('Link Following') vulnerability [CWE-59] vulnerability in Fortinet FortiClientWindows 7.4.0 through 7.4.4, FortiClientWindows 7.2.0 through 7.2.12, FortiClientWindows 7.0 all versions may allow a local low-privilege attacker to perform an arbitrary file write with elevated permissions via crafted named pipe messages.	7.1	More Details
CVE-2020-37154	eLection 2.0 contains an authenticated SQL injection vulnerability in the candidate management endpoint that allows attackers to manipulate database queries through the 'id' parameter. Attackers can leverage SQLMap to exploit the vulnerability, potentially gaining remote code execution by uploading backdoor files to the web application directory.	7.1	More Details
CVE-2020-37147	ATutor 2.2.4 contains a SQL injection vulnerability in the admin user deletion page that allows authenticated attackers to manipulate database queries through the 'id' parameter. Attackers can exploit the vulnerability by injecting malicious SQL code into the 'id' parameter of the admin_delete.php script to potentially extract or modify database information.	7.1	More Details
CVE-2026-25536	MCP TypeScript SDK is the official TypeScript SDK for Model Context Protocol servers and clients. From version 1.10.0 to 1.25.3, cross-client response data leak when a single McpServer/Server and transport instance is reused across multiple client connections, most commonly in stateless StreamableHTTPServerTransport deployments. This issue has been patched in version 1.26.0.	7.1	More Details
CVE-2025-11142	The VAPIX API mediaclip.cgi that did not have a sufficient input validation allowing for a possible remote code execution. This flaw can only be exploited after authenticating with an operator- or administrator- privileged service account.	7.1	More Details
CVE-2026-21517	Improper link resolution before file access ('link following') in Windows App for Mac allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2025-15569	A flaw has been found in Artifex MuPDF up to 1.26.1 on Windows. The impacted element is the function get_system_dpi of the file platform/x11/win_main.c. This manipulation causes uncontrolled search path. The attack requires local access. The attack is considered to have high complexity. The exploitability is regarded as difficult. Upgrading to version 1.26.2 is sufficient to resolve this issue. Patch name: ebb125334eb007d64e579204af3c264aadf2e244. Upgrading the affected component is recommended.	7.0	More Details
CVE-2026-21242	Use after free in Windows Subsystem for Linux allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-21508	Improper authentication in Windows Storage allows an authorized attacker to elevate privileges locally.	7.0	More Details

CVE-2026-21237	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Subsystem for Linux allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-21253	Use after free in Mailslot File System allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-21241	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-21234	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Connected Devices Platform Service allows an authorized attacker to elevate privileges locally.	7.0	More Details
CVE-2026-24922	Buffer overflow vulnerability in the HDC module. Impact: Successful exploitation of this vulnerability may affect availability.	6.9	More Details
CVE-2026-20980	Improper input validation in PACM prior to SMR Feb-2026 Release 1 allows physical attacker to execute arbitrary commands.	6.8	More Details
CVE-2026-24918	Address read vulnerability in the communication module. Impact: Successful exploitation of this vulnerability may affect availability.	6.8	More Details
CVE-2025-7708	Insertion of Sensitive Information Into Sent Data vulnerability in Atlas Educational Software Industry Ltd. Co. K12net allows Communication Channel Manipulation.This issue affects k12net: through 09022026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.8	More Details
CVE-2025-20080	Null pointer dereference in the firmware for some Intel(R) AMT and Intel(R) Standard Manageability within Ring 0: Kernel may allow a denial of service. Network adversary with an unauthenticated user combined with a high complexity attack may enable denial of service. This result may potentially occur via network access when attack requirements are present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (none), integrity (none) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.8	More Details
CVE-2025-31990	Rate limiting for certain API calls is not being enforced, making HCL Velocity vulnerable to Denial of Service (DoS) attacks. An attacker could flood the system with a large number of requests, overwhelming its resources and causing it to become unresponsive to legitimate users. This vulnerability is fixed in 5.1.7.	6.8	More Details
CVE-2026-24777	OpenProject is an open-source, web-based project management software. Prior to 17.0.2, users with the Manage Users permission can lock and unlock users. This functionality should only be possible for users of the application, but they were not supposed to be able to lock application administrators. Due to a missing permission check this logic was not enforced. The problem was fixed in OpenProject 17.0.2The problem was fixed in OpenProject 17.0.2.	6.7	More Details
CVE-2025-14740	Docker Desktop for Windows contains multiple incorrect permission assignment vulnerabilities in the installer's handling of the C:\ProgramData\DockerDesktop directory. The installer creates this directory without proper ownership verification, creating two exploitation scenarios: Scenario 1 (Persistent Attack): If a low-privileged attacker pre-creates C:\ProgramData\DockerDesktop before Docker Desktop installation, the attacker retains ownership of the directory even after the installer applies restrictive ACLs. At any time after installation completes, the attacker can modify the directory ACL (as the owner) and tamper with critical configuration files such as install-settings.json to specify a malicious credentialHelper, causing arbitrary code execution when any user runs Docker Desktop. Scenario 2 (TOCTOU Attack): During installation, there is a time-of-check-time-of-use	6.7	More Details

	(TOCTOU) race condition between when the installer creates C:\ProgramData\DockerDesktop and when it sets secure ACLs. A low-privileged attacker actively monitoring for the installation can inject malicious files (such as install-settings.json) with attacker-controlled ACLs during this window, achieving the same code execution outcome.		
CVE-2025-36511	Incorrect default permissions for some Intel(R) Memory and Storage Tool before version 2.5.2 within Ring 3: User Applications may allow an escalation of privilege. System software adversary with an authenticated user combined with a high complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires active user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.7	More Details
CVE-2025-15316	Tanium addressed a local privilege escalation vulnerability in Tanium Server.	6.7	More Details
CVE-2025-20070	Improper conditions check for the Intel(R) Optane(TM) PMem management software before versions CR_MGMT_02.00.00.4052, CR_MGMT_03.00.00.0538 within Ring 3: User Applications may allow an escalation of privilege. Unprivileged software adversary with an authenticated user combined with a high complexity attack may enable [cvss_threat_loss_factor]. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires active user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.7	More Details
CVE-2025-32092	Insecure inherited permissions for some Intel(R) Graphics Software before version 25.30.1702.0 within Ring 3: User Applications may allow an escalation of privilege. Unprivileged software adversary with an authenticated user combined with a high complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires active user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.7	More Details
CVE-2025-31655	Incorrect default permissions for some Intel(R) Battery Life Diagnostic Tool within Ring 3: User Applications may allow an escalation of privilege. Unprivileged software adversary with an authenticated user combined with a high complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires active user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.7	More Details
CVE-2025-15315	Tanium addressed a local privilege escalation vulnerability in Tanium Module Server.	6.7	More Details
CVE-2025-22849	Incorrect default permissions for the Intel(R) Optane(TM) PMem management software before versions CR_MGMT_01.00.00.3584, CR_MGMT_02.00.00.4052, CR_MGMT_03.00.00.0538 within Ring 3: User Applications may allow an escalation of privilege. Unprivileged software adversary with an authenticated user combined with a high complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires active user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.7	More Details
	Uncontrolled search path in some software installer for some VTune(TM) Profiler software		

CVE-2025-20106	and Intel(R) oneAPI Base Toolkits before version 2025.0. within Ring 3: User Applications may allow an escalation of privilege. System software adversary with an authenticated user combined with a high complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires active user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.7	More Details
CVE-2025-36522	Incorrect default permissions for some Intel(R) Chipset Software before version 10.1.20266.8668 or later. within Ring 3: User Applications may allow an escalation of privilege. System software adversary with an authenticated user combined with a high complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires active user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.7	More Details
CVE-2025-32452	Uncontrolled search path for some AI Playground before version 2.6.1 beta within Ring 3: User Applications may allow an escalation of privilege. Unprivileged software adversary with an authenticated user combined with a high complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires active user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.7	More Details
CVE-2025-32453	Incorrect default permissions for some Intel(R) Graphics Driver software within Ring 2: Privileged Process may allow an escalation of privilege. Unprivileged software adversary with an authenticated user combined with a high complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires active user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.7	More Details
CVE-2025-35999	Incorrect permission assignment for critical resource for some System Firmware Update Utility (SysFwUpdt) for Intel(R) Server Boards and Intel(R) Server Systems Based before version 16.0.12. within Ring 3: User Applications may allow an escalation of privilege. System software adversary with a privileged user combined with a low complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires passive user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.7	More Details
CVE-2025-64157	A use of externally-controlled format string vulnerability in Fortinet FortiOS 7.6.0 through 7.6.4, FortiOS 7.4.0 through 7.4.9, FortiOS 7.2.0 through 7.2.11, FortiOS 7.0 all versions allows an authenticated admin to execute unauthorized code or commands via specifically crafted configuration.	6.7	More Details
CVE-2026-21522	Improper neutralization of special elements used in a command ('command injection') in Azure Compute Gallery allows an authorized attacker to elevate privileges locally.	6.7	More Details
CVE-2025-15312	Tanium addressed an improper output sanitization vulnerability in Tanium Appliance.	6.6	More Details
CVE-2026-21419	Dell Display and Peripheral Manager (Windows) versions prior to 2.2 contain an Improper Link Resolution Before File Access ('Link Following') vulnerability in the Installer and Service. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of Privileges	6.6	More Details

CVE-2025-15324	Tanium addressed a documentation issue in Engage.	6.6	More Details
CVE-2026-25749	Vim is an open source, command line text editor. Prior to version 9.1.2132, a heap buffer overflow vulnerability exists in Vim's tag file resolution logic when processing the 'helpfile' option. The vulnerability is located in the get_tagfname() function in src/tag.c. When processing help file tags, Vim copies the user-controlled 'helpfile' option value into a fixed-size heap buffer of MAXPATHL + 1 bytes (typically 4097 bytes) using an unsafe STRCPY() operation without any bounds checking. This issue has been patched in version 9.1.2132.	6.6	More Details
CVE-2026-20981	Improper input validation in FacAtFunction prior to SMR Feb-2026 Release 1 allows privileged physical attacker to execute arbitrary command with system privilege.	6.6	More Details
CVE-2026-26006	AutoGPT is a platform that allows users to create, deploy, and manage continuous artificial intelligence agents that automate complex workflows. The autogpt before 0.6.32 is vulnerable to Regular Expression Denial of Service due to the use of regex at Code Extraction Block. The two Regex are used containing the corresponding dangerous patterns \s+[\s\S]*? and \s+(.*?). They share a common characteristic — the combination of two adjacent quantifiers that can match the same space character (\s). As a result, an attacker can supply a long sequence of space characters to trigger excessive regex backtracking, potentially leading to a Denial of Service (DoS). This vulnerability is fixed in 0.6.32.	6.5	More Details
CVE-2025-69216	OpenSTAManager is an open source management software for technical assistance and invoicing. In 2.9.8 and earlier, an authenticated SQL injection vulnerability in OpenSTAManager's Scadenzario (Payment Schedule) print template allows any authenticated user to extract sensitive data from the database, including admin credentials, customer information, and financial records. The vulnerability exists in templates/scadenzario/init.php, where the id_anagrafica parameter is directly concatenated into an SQL query without proper sanitization. The vulnerability enables complete database read access through error-based SQL injection techniques.	6.5	More Details
CVE-2026-24417	OpenSTAManager is an open source management software for technical assistance and invoicing. OpenSTAManager v2.9.8 and earlier contain a critical Time-Based Blind SQL Injection vulnerability in the global search functionality. The application fails to properly sanitize the term parameter before using it in SQL LIKE clauses across multiple module-specific search handlers, allowing attackers to inject arbitrary SQL commands and extract sensitive data through time-based Boolean inference.	6.5	More Details
CVE-2026-24416	OpenSTAManager is an open source management software for technical assistance and invoicing. OpenSTAManager v2.9.8 and earlier contain a critical Time-Based Blind SQL Injection vulnerability in the article pricing completion handler. The application fails to properly sanitize the idarticolo parameter before using it in SQL queries, allowing attackers to inject arbitrary SQL commands and extract sensitive data through time-based Boolean inference.	6.5	More Details
CVE-2026-25613	An authorized user may disable the MongoDB server by issuing a query against a collection that contains an invalid compound wildcard index.	6.5	More Details
CVE-2025-15260	The MyRewards – Loyalty Points and Rewards for WooCommerce plugin for WordPress is vulnerable to missing authorization in all versions up to, and including, 5.6.0. This is due to the plugin not properly verifying that a user is authorized to perform an action in the 'ajax' function. This makes it possible for authenticated attackers, with subscriber level access and above, to modify, add, or delete loyalty program earning rules, including manipulating point multipliers to arbitrary values.	6.5	More Details
CVE-2026-25610	An authorized user may trigger a server crash by running a $geoNear pipeline with certain invalid index hints.	6.5	More Details
	OpenSTAManager is an open source management software for technical assistance and invoicing. OpenSTAManager v2.9.8 and earlier contain a critical Error-Based SQL Injection		

CVE-2026-24418	vulnerability in the bulk operations handler for the Scadenzario (Payment Schedule) module. The application fails to validate that elements of the id_records array are integers before using them in an SQL IN() clause, allowing attackers to inject arbitrary SQL commands and extract sensitive data through XPATH error messages.	6.5	More Details
CVE-2026-2302	Under specific conditions when processing a maliciously crafted value of type Hash r, Mongoid::Criteria.from_hash may allow for executing arbitrary Ruby code.	6.5	More Details
CVE-2026-1495	The vulnerability, if exploited, could allow an attacker with Event Log Reader (S-1-5-32-573) privileges to obtain proxy details, including URL and proxy credentials, from the PI to CONNECT event log files. This could enable unauthorized access to the proxy server.	6.5	More Details
CVE-2025-15477	The Bucketlister plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode `category` and `id` attributes in all versions up to, and including, 0.1.5 due to insufficient escaping on the user supplied parameters and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	6.5	More Details
CVE-2026-25540	Mastodon is a free, open-source social network server based on ActivityPub. Prior to versions 4.3.19, 4.4.13, 4.5.6, Mastodon is vulnerable to web cache poisoning via `Rails.cache. When AUTHORIZED_FETCH is enabled, the ActivityPub endpoints for pinned posts and featured hashtags have contents that depend on the account that signed the HTTP request. However, these contents are stored in an internal cache and reused with no regards to the signing actor. As a result, an empty response generated for a blocked user account may be served to requests from legitimate non-blocked actors, or conversely, content intended for non-blocked actors may be returned to blocked actors. This issue has been patched in versions 4.3.19, 4.4.13, 4.5.6.	6.5	More Details
CVE-2026-24900	MarkUs is a web application for the submission and grading of student assignments. Prior to 2.9.1, the courses/<:course_id>/assignments/<:assignment_id>/submissions/html_content accepted a select_file_id parameter to serve SubmissionFile objects containing a record of files submitted by students. This parameter was not correctly scoped to the requesting user, allowing users access arbitrary submission file contents by id. This vulnerability is fixed in 2.9.1.	6.5	More Details
CVE-2026-2303	The mongo-go-driver repository contains CGo bindings for GSSAPI (Kerberos) authentication on Linux and macOS. The C wrapper implementation contains a heap out-of-bounds read vulnerability due to incorrect assumptions about string termination in the GSSAPI standard. Since GSSAPI buffers are not guaranteed to be null-terminated or have extra padding, this results in reading one byte past the allocated heap buffer.	6.5	More Details
CVE-2026-25957	Cube is a semantic layer for building data applications. From 1.1.17 to before 1.5.13 and 1.4.2, it is possible to make the entire Cube API unavailable by submitting a specially crafted request to a Cube API endpoint. This vulnerability is fixed in 1.5.13 and 1.4.2.	6.5	More Details
CVE-2026-25723	Claude Code is an agentic coding tool. Prior to version 2.0.55, Claude Code failed to properly validate commands using piped sed operations with the echo command, allowing attackers to bypass file write restrictions. This vulnerability enabled writing to sensitive directories like the .claude folder and paths outside the project scope. Exploiting this required the ability to execute commands through Claude Code with the "accept edits" feature enabled. This issue has been patched in version 2.0.55.	6.5	More Details
CVE-2025-15317	Tanium addressed an uncontrolled resource consumption vulnerability in Tanium Server.	6.5	More Details
CVE-2026-25479	Litestar is an Asynchronous Server Gateway Interface (ASGI) framework. Prior to 2.20.0, in litestar.middleware.allowed_hosts, allowlist entries are compiled into regex patterns in a way that allows regex metacharacters to retain special meaning (e.g., . matches any character). This enables a bypass where an attacker supplies a host that matches the regex but is not the intended literal hostname. This vulnerability is fixed in 2.20.0.	6.5	More Details

CVE-2026-24419	OpenSTAManager is an open source management software for technical assistance and invoicing. OpenSTAManager v2.9.8 and earlier contain a critical Error-Based SQL Injection vulnerability in the Prima Nota (Journal Entry) module's add.php file. The application fails to validate that comma-separated values from the id_documenti GET parameter are integers before using them in SQL IN() clauses, allowing attackers to inject arbitrary SQL commands and extract sensitive data through XPATH error messages.	6.5	More Details
CVE-2026-23633	Gogs is an open source self-hosted Git service. In version 0.13.3 and prior, there is an arbitrary file read/write via path traversal in Git hook editing. This issue has been patched in versions 0.13.4 and 0.14.0+dev.	6.5	More Details
CVE-2026-23632	Gogs is an open source self-hosted Git service. In version 0.13.3 and prior, the endpoint "PUT /repos/:owner/:repo/contents/*" does not require write permissions and allows access with read permission only via repoAssignment(). After passing the permission check, PutContents() invokes UpdateRepoFile(), which results in commit creation and the execution of git push. As a result, a token with read-only permission can be used to modify repository contents. This issue has been patched in versions 0.13.4 and 0.14.0+dev.	6.5	More Details
CVE-2026-22592	Gogs is an open source self-hosted Git service. In version 0.13.3 and prior, an authenticated user can cause a DOS attack. If one of the repo files is deleted before synchronization, it will cause the application to crash. This issue has been patched in versions 0.13.4 and 0.14.0+dev.	6.5	More Details
CVE-2024-51451	IBM Concert 1.0.0 through 2.1.0 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking.	6.5	More Details
CVE-2026-24917	UAF vulnerability in the security module. Impact: Successful exploitation of this vulnerability may affect availability.	6.5	More Details
CVE-2026-1850	Complex queries can cause excessive memory usage in MongoDB Query Planner resulting in an Out-Of-Memory Crash.	6.5	More Details
CVE-2026-0484	Due to missing authorization check in SAP NetWeaver Application Server ABAP and SAP S/4HANA, an authenticated attacker could access a specific transaction code and modify the text data in the system. This vulnerability has a high impact on integrity of the application with no effect on the confidentiality and availability.	6.5	More Details
CVE-2026-21512	Server-side request forgery (ssrf) in Azure DevOps Server allows an authorized attacker to perform spoofing over a network.	6.5	More Details
CVE-2026-1602	SQL injection in Ivanti Endpoint Manager before version 2024 SU5 allows a remote authenticated attacker to read arbitrary data from the database.	6.5	More Details
CVE-2026-25846	In JetBrains YouTrack before 2025.3.119033 access tokens could be exposed in Mailbox logs	6.5	More Details
CVE-2026-24098	Apache Airflow versions before 3.1.7, has vulnerability that allows authenticated UI users with permission to one or more specific Dags to view import errors generated by other Dags they did not have access to. Users are advised to upgrade to 3.1.7 or later, which resolves this issue	6.5	More Details
CVE-2026-22922	Apache Airflow versions 3.1.0 through 3.1.6 contain an authorization flaw that can allow an authenticated user with custom permissions limited to task access to view task logs without having task log access. Users are recommended to upgrade to Apache Airflow 3.1.7 or later, which resolves this issue.	6.5	More Details
	Improper authorization in the Intel(R) Quick Assist Technology for some Intel(R) Platforms		

CVE-2025-30508	within Ring 0: Kernel may allow a denial of service. Unprivileged software adversary with an authenticated user combined with a low complexity attack may enable denial of service. This result may potentially occur via local access when attack requirements are not present with special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (none), integrity (none) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.5	More Details
CVE-2026-2235	C&Cm@il developed by HGiga has a SQL Injection vulnerability, allowing authenticated remote attackers to inject arbitrary SQL commands to read database contents.	6.5	More Details
CVE-2026-0391	User interface (ui) misrepresentation of critical information in Microsoft Edge for Android allows an unauthorized attacker to perform spoofing over a network.	6.5	More Details
CVE-2025-32003	Out-of-bounds read in the firmware for some 100GbE Intel(R) Ethernet Network Adapter E810 before version cvl fw 1.7.6, cpk 1.3.7 within Ring 0: Bare Metal OS may allow a denial of service. Network adversary with an authenticated user combined with a low complexity attack may enable denial of service. This result may potentially occur via network access when attack requirements are present with special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (none), integrity (none) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.5	More Details
CVE-2026-25760	Sliver is a command and control framework that uses a custom Wireguard netstack. Prior to 1.6.11, a path traversal in the website content subsystem lets an authenticated operator read arbitrary files on the Sliver server host. This is an authenticated path traversal / arbitrary file read issue, and it can expose credentials, configs, and keys. This vulnerability is fixed in 1.6.11.	6.5	More Details
CVE-2025-15343	Tanium addressed an incorrect default permissions vulnerability in Enforce.	6.5	More Details
CVE-2025-15341	Tanium addressed an incorrect default permissions vulnerability in Benchmark.	6.5	More Details
CVE-2025-15340	Tanium addressed an incorrect default permissions vulnerability in Comply.	6.5	More Details
CVE-2025-15339	Tanium addressed an incorrect default permissions vulnerability in Discover.	6.5	More Details
CVE-2025-15338	Tanium addressed an incorrect default permissions vulnerability in Partner Integration.	6.5	More Details
CVE-2025-15337	Tanium addressed an incorrect default permissions vulnerability in Patch.	6.5	More Details
CVE-2025-15336	Tanium addressed an incorrect default permissions vulnerability in Performance.	6.5	More Details
CVE-2026-21518	Improper neutralization of special elements used in a command ('command injection') in GitHub Copilot and Visual Studio Code allows an unauthorized attacker to bypass a security feature over a network.	6.5	More Details
CVE-	User interface (ui) misrepresentation of critical information in Microsoft Exchange Server		More

2026-21527	allows an unauthorized attacker to perform spoofing over a network.	6.5	Details
CVE-2026-21528	Binding to an unrestricted ip address in Azure IoT SDK allows an unauthorized attacker to disclose information over a network.	6.5	More Details
CVE-2026-23655	Cleartext storage of sensitive information in Azure Compute Gallery allows an authorized attacker to disclose information over a network.	6.5	More Details
CVE-2026-1849	MongoDB Server may experience an out-of-memory failure while evaluating expressions that produce deeply nested documents. The issue arises in recursive functions because the server does not periodically check the depth of the expression.	6.5	More Details
CVE-2026-0572	The WebPurify Profanity Filter plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'webpurify_save_options' function in all versions up to, and including, 4.0.2. This makes it possible for unauthenticated attackers to change plugin settings.	6.5	More Details
CVE-2026-1847	Inserting certain large documents into a replica set could lead to replica set secondaries not being able to fetch the oplog from the primary. This could stall replication inside the replica set leading to server crash.	6.5	More Details
CVE-2026-25565	WeKan versions prior to 8.19 contain an authorization vulnerability where certain card update API paths validate only board read access rather than requiring write permission. This can allow users with read-only roles to perform card updates that should require write access.	6.5	More Details
CVE-2026-0948	Authentication Bypass Using an Alternate Path or Channel vulnerability in Drupal Microsoft Entra ID SSO Login allows Privilege Escalation.This issue affects Microsoft Entra ID SSO Login: from 0.0.0 before 1.0.4.	6.5	More Details
CVE-2026-24324	SAP BusinessObjects Business Intelligence Platform (AdminTools) allows an authenticated attacker with user privileges to execute a specific query in AdminTools that could cause the Content Management Server (CMS) to crash, rendering the CMS partially or completely unavailable and resulting in the denial of service of the Content Management Server (CMS). Successful exploitation impacts system availability, while confidentiality and integrity remain unaffected.	6.5	More Details
CVE-2026-25480	Litestar is an Asynchronous Server Gateway Interface (ASGI) framework. Prior to 2.20.0, FileStore maps cache keys to filenames using Unicode NFKD normalization and ord() substitution without separators, creating key collisions. When FileStore is used as response-cache backend, an unauthenticated remote attacker can trigger cache key collisions via crafted paths, causing one URL to serve cached responses of another (cache poisoning/mixup). This vulnerability is fixed in 2.20.0.	6.5	More Details
CVE-2026-25475	OpenClaw is a personal AI assistant. Prior to version 2026.1.30, the isValidMedia() function in src/media/parse.ts allows arbitrary file paths including absolute paths, home directory paths, and directory traversal sequences. An agent can read any file on the system by outputting MEDIA:/path/to/file, exfiltrating sensitive data to the user/channel. This issue has been patched in version 2026.1.30.	6.5	More Details
CVE-2025-14150	IBM webMethods Integration (on prem) - Integration Server 10.15 through IS_10.15_Core_Fix2411.1 to IS_11.1_Core_Fix8 IBM webMethods Integration could disclose sensitive user information in server responses.	6.5	More Details
CVE-2026-25612	The internal locking mechanism of the MongoDB server uses an internal encoding of the resources in order to choose what lock to take. Collections may inadvertently collide with one another in this representation causing unavailability between them due to conflicting locks.	6.5	More Details
CVE-2025-	Crafted delegations or IP fragments can poison cached delegations in Recursor.	6.5	More

59024			Details
CVE-2025-68699	NanoMQ MQTT Broker (NanoMQ) is an all-around Edge Messaging Platform. In version 0.24.6, NanoMQ has a protocol parsing / forwarding inconsistency when handling shared subscriptions ($share/). A malformed SUBSCRIBE topic such as $share/ab (missing the second /) is not strictly validated during the subscription stage, so the invalid Topic Filter is stored into the subscription table. Later, when any PUBLISH matches this subscription, the broker send path (nmq_pipe_send_start_v4/v5) performs a second $share/ parsing using strchr() and increments the returned pointer without NULL checks. If the second strchr() returns NULL, sub_topic++ turns the pointer into an invalid address (e.g. 0x1). This invalid pointer is then passed into topic_filtern(), which triggers strlen() and crashes with SIGSEGV. The crash is stable and remotely triggerable. This issue has been patched in version 0.24.7.	6.5	More Details
CVE-2026-22044	GLPI is a free asset and IT management software package. From version 0.85 to before 10.0.23, an authenticated user can perform a SQL injection. This issue has been patched in version 10.0.23.	6.5	More Details
CVE-2025-10464	Insecure Storage of Sensitive Information vulnerability in Birtech Information Technologies Industry and Trade Ltd. Co. Senseway allows Retrieve Embedded Sensitive Data.This issue affects Senseway: through 09022026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.5	More Details
CVE-2026-1570	The Simple Bible Verse via Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's `verse` shortcode in all versions up to, and including, 1.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2025-15267	The Bold Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's bt_bb_accordion_item shortcode in all versions up to, and including, 5.5.7 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-2025-12159	The Bold Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's bt_bb_raw_content shortcode in all versions up to, and including, 5.4.8 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-2025-12803	The Bold Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin 'bt_bb_tabs' shortcode in all versions up to, and including, 5.5.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-0555	The Premmerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'premmerce_wizard_actions' AJAX endpoint in all versions up to, and including, 1.3.20. This is due to missing capability checks and insufficient input sanitization and output escaping on the `state` parameter. This makes it possible for authenticated attackers, with subscriber level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page (the Premmerce Wizard admin page).	6.4	More Details
CVE-2025-13463	The Bold Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Post Grid component in all versions up to, and including, 5.5.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-1573	The OMIGO plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's `omigo_donate_button` shortcode in all versions up to, and including, 3.3 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	6.4	More Details

	scripts in pages that will execute whenever a user accesses an injected page.		
CVE-2026-1608	The Video Onclick plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's `youtube` shortcode in all versions up to, and including, 0.4.7 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-2026-1252	The Events Listing Widget plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Event URL' parameter in all versions up to, and including, 1.3.4 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 an injected page.	6.4	More Details
CVE-2026-0742	The Smart Appointment & Booking plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the saab_save_form_data AJAX action in all versions up to, and including, 1.0.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-25805	Zed is a multiplayer code editor. Prior to 0.219.4, Zed does not show with which parameters a tool is being invoked, when asking for allowance. Further it does not show after the tool was being invoked, which parameters were used. Thus, maybe unwanted or even malicious values could be used without the user having a chance to notice it. Patched in Zed Editor 0.219.4 which includes expandable tool call details.	6.4	More Details
CVE-2026-1922	The The Events Calendar Shortcode & Block plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's `ecs-list-events` shortcode `message` attribute in all versions up to, and including, 3.1.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-0996	The Fluent Forms plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the AI Form Builder module in all versions up to, and including, 6.1.14 due to a combination of missing authorization checks, a leaked nonce, and insufficient input sanitization. The vulnerability allows Subscriber-level users to trigger AI form generation via a protected endpoint. When prompted, AI services will typically return bare JavaScript code (without <script> tags), which bypasses the plugin's sanitization. This stored JavaScript executes whenever anyone views the generated form, making it possible for authenticated attackers with Subscriber-level access and above to inject arbitrary web scripts that will execute in the context of any user accessing the form.	6.4	More Details
CVE-2026-0867	The Essential Widgets plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's ew-author, ew-archive, ew-category, ew-page, and ew-menu shortcodes in all versions up to, and including, 3.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. NOTE: This vulnerability was partially fixed in version 3.0.	6.4	More Details
CVE-2026-1268	The Dynamic Widget Content plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the widget content field in the Gutenberg editor sidebar in all versions up to, and including, 1.3.6 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-	The Tune Library plugin for WordPress is vulnerable to Stored Cross-Site Scripting via CSV import in all versions up to, and including, 1.6.3. This is due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the injected page. The vulnerability exists	6.4	More Details

1401	that will execute whenever a user accesses the injected page. The vulnerability exists because the CSV import functionality lacks authorization checks and doesn't sanitize imported data, which is later rendered without escaping through the [tune-library] shortcode.		Details
CVE-2026-1808	The Orange Confort+ accessibility toolbar for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'style' parameter of the ocplus_button shortcode in all versions up to, and including, 0.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-1888	The Docus – YouTube Video Playlist plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'docusplaylist' shortcode in all versions up to, and including, 1.0.6 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-2026-1909	The WaveSurfer-WP plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's audio shortcode in all versions up to, and including, 2.8.3 due to insufficient input sanitization and output escaping on the 'src' attribute. 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-2026-1611	The Wikiloops Track Player plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's `wikiloops` shortcode in all versions up to, and including, 1.0.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-1279	The Employee Directory plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'form_title' parameter in the `search_employee_directory` shortcode in all versions up to, and including, 1.2.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with 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-2026-1319	The Robin Image Optimizer – Unlimited Image Optimization & WebP Converter plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Alternative Text' field of a Media Library image in all versions up to, and including, 2.0.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-1293	The Yoast SEO – Advanced SEO with real-time guidance and built-in AI plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the the `yoast-schema` block attribute in all versions up to, and including, 26.8 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-2019-25301	Millhouse-Project 1.414 contains a persistent cross-site scripting vulnerability in the comment submission functionality that allows attackers to inject malicious scripts. Attackers can post comments with embedded JavaScript through the 'content' parameter in add_comment_sql.php to execute arbitrary scripts in victim browsers.	6.4	More Details
CVE-2019-25294	html5_snmp 1.11 contains a persistent cross-site scripting vulnerability that allows attackers to inject malicious scripts through the 'Remark' parameter in add_router_operation.php. Attackers can craft a POST request with a script payload in the Remark field to execute arbitrary JavaScript in victim browsers when the page is loaded.	6.4	More Details
CVE-	The Wonka Slide plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's `list_class` shortcode in all versions up to, and including, 1.3.3 due to insufficient		More

2026-1613	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	Details
CVE-2026-2078	A vulnerability was detected in yeqifu warehouse up to aaf29962ba407d22d991781de28796ee7b4670e4. This affects the function addPermission/updatePermission/deletePermission of the file dataset\repos\warehouse\src\main\java\com\yeqifu\sys\controller\PermissionController.java of the component Permission Management. Performing a manipulation results in improper authorization. The attack may be initiated remotely. The exploit is now public and may be used. This product uses a rolling release model to deliver continuous updates. As a result, specific version information for affected or updated releases is not available. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-2077	A security vulnerability has been detected in yeqifu warehouse up to aaf29962ba407d22d991781de28796ee7b4670e4. Affected by this issue is the function addRole/updateRole/deleteRole of the file dataset\repos\warehouse\src\main\java\com\yeqifu\sys\controller\RoleController.java of the component Role Management Handler. Such manipulation leads to improper authorization. The attack can be launched remotely. The exploit has been disclosed publicly and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-2079	A flaw has been found in yeqifu warehouse up to aaf29962ba407d22d991781de28796ee7b4670e4. This vulnerability affects the function addMenu/updateMenu/deleteMenu of the file dataset\repos\warehouse\src\main\java\com\yeqifu\sys\controller\MenuController.java of the component Menu Management. Executing a manipulation can lead to improper authorization. The attack may be launched remotely. The exploit has been published 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.	6.3	More Details
CVE-2026-2076	A weakness has been identified in yeqifu warehouse up to aaf29962ba407d22d991781de28796ee7b4670e4. Affected by this vulnerability is the function addUser/updateUser/deleteUser of the file dataset\repos\warehouse\src\main\java\com\yeqifu\sys\controller\UserController.java of the component User Management Endpoint. This manipulation causes improper authorization. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-2169	A vulnerability has been found in D-Link DWR-M921 1.1.50. This impacts an unknown function of the file /boafrm/formLtefotaUpgradeFibocom. Such manipulation of the argument fota_url leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2026-2105	A flaw has been found in yeqifu warehouse up to aaf29962ba407d22d991781de28796ee7b4670e4. The affected element is the function addDept/updateDept/deleteDept of the file dataset\repos\warehouse\src\main\java\com\yeqifu\sys\controller\DeptController.java of the component Department Management. Executing a manipulation can lead to improper authorization. It is possible to launch the attack remotely. The exploit has been published and may be used. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
	A vulnerability was determined in D-Link DCS-933L up to 1.14.11. This affects an unknown		

CVE-2026-2218	function of the file /setSystemAdmin of the component alphapd. This manipulation of the argument AdminID causes command injection. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized. This vulnerability only affects products that are no longer supported by the maintainer.	6.3	More Details
CVE-2026-2194	A flaw has been found in D-Link DI-7100G C1 24.04.18D1. This affects the function start_proxy_client_email. Executing a manipulation can lead to command injection. The attack can be executed remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2026-2193	A vulnerability was detected in D-Link DI-7100G C1 24.04.18D1. Affected by this issue is the function set_jhttpd_info. Performing a manipulation of the argument usb_username results in command injection. Remote exploitation of the attack is possible.	6.3	More Details
CVE-2026-2183	A security vulnerability has been detected in Great Developers Certificate Generation System up to 97171bb0e5e22e52eacf4e4fa81773e5f3cffb73. This affects an unknown part of the file /restructured/csv.php. The manipulation leads to unrestricted upload. Remote exploitation of the attack is possible. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided. The code repository of the project has not been active for many years.	6.3	More Details
CVE-2026-2178	A vulnerability was found in r-huijts xcode-mcp-server up to f3419f00117aa9949e326f78cc940166c88f18cb. This affects the function registerXcodeTools of the file src/tools/xcode/index.ts of the component run_lldb. The manipulation of the argument args results in command injection. It is possible to launch the attack remotely. The exploit has been made public and could be used. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available. The patch is identified as 11f8d6bacadd153beee649f92a78a9dad761f56f. Applying a patch is advised to resolve this issue.	6.3	More Details
CVE-2026-2176	A security vulnerability has been detected in code-projects Contact Management System 1.0. This issue affects some unknown processing of the file index.py. Such manipulation of the argument selecteditem[0] leads to sql injection. The attack can be executed remotely.	6.3	More Details
CVE-2026-2122	A security flaw has been discovered in Xiaopi Panel up to 20260126. This impacts an unknown function of the file /demo.php of the component WAF Firewall. 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. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-2168	A flaw has been found in D-Link DWR-M921 1.1.50. This affects the function sub_419920 of the file /boafrm/formLtefotaUpgradeQuectel. This manipulation of the argument fota_url causes command injection. It is possible to initiate the attack remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2026-2074	A vulnerability was identified in O2OA up to 9.0.0. This impacts an unknown function of the file /x_program_center/jaxrs/mpweixin/check of the component HTTP POST Request Handler. The manipulation leads to xml external entity reference. It is possible to initiate 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.	6.3	More Details
CVE-2026-2146	A security flaw has been discovered in guchengwuyue yshopmall up to 1.9.1. This affects the function updateAvatar of the file /api/users/updateAvatar of the component co.yixiang.utils.FileUtil. Performing a manipulation of the argument File results in unrestricted upload. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-2141	A security flaw has been discovered in WuKongOpenSource WukongCRM up to 11.3.3. This affects an unknown part of the file gateway/src/main/java/com/kakarote/gateway/service/impl/PermissionServiceImpl.java of the component URL Handler. Performing a manipulation results in improper authorization. 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	6.3	More Details

	not respond in any way.		
CVE-2026-2075	A security flaw has been discovered in yeqifu warehouse up to aaf29962ba407d22d991781de28796ee7b4670e4. Affected is the function saveRolePermission of the file dataset\repos\warehouse\src\main\java\com\yeqifu\sys\controller\RoleController.java of the component Role-Permission Binding Handler. The manipulation results in improper access controls. It is possible to launch the attack remotely. The exploit has been released to the public and may be used for attacks. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-2106	A vulnerability has been found in yeqifu warehouse up to aaf29962ba407d22d991781de28796ee7b4670e4. The impacted element is the function addNotice/updateNotice/deleteNotice/batchDeleteNotice of the file dataset\repos\warehouse\src\main\java\com\yeqifu\sys\controller\NoticeController.java of the component Notice Management. The manipulation leads to improper authorization. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-2107	A vulnerability was found in yeqifu warehouse up to aaf29962ba407d22d991781de28796ee7b4670e4. This affects the function loadAllLoginfo/deleteLoginfo/batchDeleteLoginfo of the file dataset\repos\warehouse\src\main\java\com\yeqifu\sys\controller\LoginfoController.java of the component Log Info Handler. The manipulation results in improper authorization. The attack can be launched remotely. The exploit has been made public and could be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-2135	A vulnerability was detected in UTT HiPER 810 1.7.4-141218. The impacted element is the function sub_43F020 of the file /goform/formPdbUpConfig. Performing a manipulation of the argument policyNames results in command injection. It is possible to initiate the attack remotely. The exploit is now public and may be used.	6.3	More Details
CVE-2026-2131	A vulnerability was identified in XixianLiang HarmonyOS-mcp-server 0.1.0. This vulnerability affects the function input_text. The manipulation of the argument text leads to os command injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.	6.3	More Details
CVE-2026-2130	A vulnerability was determined in BurtTheCoder mcp-maigret up to 1.0.12. This affects an unknown part of the file src/index.ts of the component search_username. Executing a manipulation of the argument Username can lead to command injection. The attack may be launched remotely. Upgrading to version 1.0.13 is able to mitigate this issue. This patch is called b1ae073c4b3e789ab8de36dc6ca8111ae9399e7a. Upgrading the affected component is advised.	6.3	More Details
CVE-2026-2209	A vulnerability was detected in WeKan up to 8.18. The affected element is the function setCreateTranslation of the file client/components/settings/translationBody.js of the component Custom Translation Handler. The manipulation results in improper authorization. The attack can be launched remotely. Upgrading to version 8.19 is sufficient to fix this issue. The patch is identified as f244a43771f6ebf40218b83b9f46dba6b940d7de. It is suggested to upgrade the affected component.	6.3	More Details
CVE-2026-2206	A security flaw has been discovered in WeKan up to 8.20. This vulnerability affects unknown code of the file server/methods/fixDuplicateLists.js of the component Administrative Repair Handler. Performing a manipulation results in improper access controls. It is possible to initiate the attack remotely. Upgrading to version 8.21 is able to resolve this issue. The patch is named 4ce181d17249778094f73d21515f7f863f554743. It is advisable to upgrade the affected component.	6.3	More Details

CVE-2026-2167	A vulnerability was detected in Totolink WA300 5.2cu.7112_B20190227. The impacted element is the function setAPNetwork of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument Ipaddr results in os command injection. The attack may be performed from remote. The exploit is now public and may be used.	6.3	More Details
CVE-2026-1813	A vulnerability was found in bolo-blog bolo-solo up to 2.6.4. Affected is an unknown function of the file src/main/java/org/b3log/solo/bolo/pic/PicUploadProcessor.java of the component FreeMarker Template Handler. The manipulation of the argument File results in unrestricted upload. It is possible to launch the attack remotely. The exploit has been made public and could be used. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-1963	A vulnerability was found in WeKan up to 8.20. This affects an unknown function of the file models/attachments.js of the component Attachment Storage. The manipulation results in improper access controls. The attack may be launched remotely. Upgrading to version 8.21 mitigates this issue. The patch is identified as c413a7e860bc4d93fe2adcf82516228570bf382d. Upgrading the affected component is advised.	6.3	More Details
CVE-2026-1962	A vulnerability has been found in WeKan up to 8.20. The impacted element is an unknown function of the file server/attachmentMigration.js of the component Attachment Migration. The manipulation leads to improper access controls. The attack may be initiated remotely. Upgrading to version 8.21 is sufficient to resolve this issue. The identifier of the patch is 053bf1dfb76ef230db162c64a6ed50ebedf67eee. It is recommended to upgrade the affected component.	6.3	More Details
CVE-2026-25508	ESF-IDF is the Espressif Internet of Things (IOT) Development Framework. In versions 5.5.2, 5.4.3, 5.3.4, 5.2.6, and 5.1.6, an out-of-bounds read vulnerability was reported in the BLE ATT Prepare Write handling of the BLE provisioning transport (protocomm_ble). The issue can be triggered by a remote BLE client while the device is in provisioning mode. The transport accumulated prepared-write fragments in a fixed-size buffer but incorrectly tracked the cumulative length. By sending repeated prepare write requests with overlapping offsets, a remote client could cause the reported length to exceed the allocated buffer size. This inflated length was then passed to provisioning handlers during execute-write processing, resulting in an out-of-bounds read and potential memory corruption. This issue has been patched in versions 5.5.3, 5.4.4, 5.3.5, 5.2.7, and 5.1.7.	6.3	More Details
CVE-2026-25507	ESF-IDF is the Espressif Internet of Things (IOT) Development Framework. In versions 5.5.2, 5.4.3, 5.3.4, 5.2.6, and 5.1.6, a use-after-free vulnerability was reported in the BLE provisioning transport (protocomm_ble) layer. The issue can be triggered by a remote BLE client while the device is in provisioning mode. The vulnerability occurred when provisioning was stopped with keep_ble_on = true. In this configuration, internal protocomm_ble state and GATT metadata were freed while the BLE stack and GATT services remained active. Subsequent BLE read or write callbacks dereferenced freed memory, allowing a connected or newly connected client to trigger invalid memory acces. This issue has been patched in versions 5.5.3, 5.4.4, 5.3.5, 5.2.7, and 5.1.7.	6.3	More Details
CVE-2026-1977	A security vulnerability has been detected in isaacwasserman mcp-vegalite-server up to 16aefed598b8cd897b78e99b907f6e2984572c61. Affected by this vulnerability is the function eval of the component visualize_data. Such manipulation of the argument vegalite_specification leads to code injection. The attack may be performed from remote. The exploit has been disclosed publicly and may be used. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated releases is not disclosed. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2026-2015	A weakness has been identified in Portabilis i-Educar up to 2.10. Affected is an unknown function of the file FinalStatusImportService.php of the component Final Status Import. Executing a manipulation of the argument school_id can lead to improper authorization. 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.	6.3	More Details

CVE-2026-24923	Permission control vulnerability in the HDC module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	6.3	More Details
CVE-2026-2065	A security flaw has been discovered in Flycatcher Toys smART Pixelator 2.0. Affected by this issue is some unknown functionality of the component Bluetooth Low Energy Interface. Performing a manipulation results in missing authentication. The attack can only be performed from the local network. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-43181	IBM Concert 1.0.0 through 2.1.0 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system.	6.3	More Details
CVE-2026-2009	A flaw has been found in SourceCodester Gas Agency Management System 1.0. This issue affects some unknown processing of the file /gasmark/php_action/createUser.php. Executing a manipulation can lead to improper access controls. It is possible to launch the attack remotely. The exploit has been published and may be used.	6.3	More Details
CVE-2026-2008	A vulnerability was detected in abhiphile fermat-mcp up to 47f11def1cd37e45dd060f30cdce346cbdbd6f0a. This vulnerability affects the function eqn_chart of the file fmcp/mpl_mcp/core/eqn_chart.py. Performing a manipulation of the argument equations results in code injection. It is possible to initiate the attack remotely. The exploit is now public and may be used. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The project was informed of the problem early through an issue report but has not responded yet.	6.3	More Details
CVE-2025-15325	Tanium addressed an improper input validation vulnerability in Discover.	6.3	More Details
CVE-2026-25532	ESF-IDF is the Espressif Internet of Things (IOT) Development Framework. In versions 5.5.2, 5.4.3, 5.3.4, 5.2.6, and 5.1.6, a vulnerability exists in the WPS (Wi-Fi Protected Setup) Enrollee implementation where malformed EAP-WSC packets with truncated payloads can cause integer underflow during fragment length calculation. When processing EAP-Expanded (WSC) messages, the code computes frag_len by subtracting header sizes from the total packet length. If an attacker sends a packet where the EAP Length field covers only the header and flags but omits the expected payload (such as the 2-byte Message Length field when WPS_MSG_FLAG_LEN is set), frag_len becomes negative. This negative value is then implicitly cast to size_t when passed to wpabuf_put_data(), resulting in a very large unsigned value. This issue has been patched in versions 5.5.3, 5.4.4, 5.3.5, 5.2.7, and 5.1.7.	6.3	More Details
CVE-2025-10258	Infinera DNA is vulnerable to a time-based SQL injection vulnerability due to insufficient input validation, which may result in leaking of sensitive information.	6.3	More Details
CVE-2026-1894	A vulnerability was detected in WeKan up to 8.20. This impacts an unknown function of the file models/checklistItems.js of the component REST API. Performing a manipulation of the argument item.cardId/item.checklistId/card.boardId results in improper authorization. Remote exploitation of the attack is possible. Upgrading to version 8.21 will fix this issue. The patch is named 251d49eea94834cf351bb395808f4a56fb4dbb44. Upgrading the affected component is recommended.	6.3	More Details
CVE-2026-1898	A vulnerability was determined in WeKan up to 8.20. This affects an unknown part of the file packages/wekan-ldap/server/syncUser.js of the component LDAP User Sync. This manipulation causes improper access controls. It is possible to initiate the attack remotely. Upgrading to version 8.21 is able to mitigate this issue. Patch name: 146905a459106b5d00b4f09453a6554255e6965a. You should upgrade the affected component.	6.3	More Details
	A vulnerability has been found in WeKan up to 8.20. Affected by this vulnerability is the		

CVE-2026-1896	A vulnerability has been found in WeKan up to 8.20. Affected by this vulnerability is the function ComprehensiveBoardMigration of the file server/migrations/comprehensiveBoardMigration.js of the component Migration Operation Handler. The manipulation of the argument boardId leads to improper access controls. The attack is possible to be carried out remotely. Upgrading to version 8.21 addresses this issue. The identifier of the patch is cc35dafef57ef6e44a514a523f9a8d891e74ad8f. Upgrading the affected component is advised.	6.3	More Details
CVE-2026-1895	A flaw has been found in WeKan up to 8.20. Affected is the function applyWipLimit of the file models/lists.js of the component Attachment Storage Handler. Executing a manipulation can lead to improper access controls. The attack can be executed remotely. Upgrading to version 8.21 is able to address this issue. This patch is called 8c0b4f79d8582932528ec2fdf2a4487c86770fb9. It is recommended to upgrade the affected component.	6.3	More Details
CVE-2026-24915	Out-of-bounds read issue in the media subsystem. Impact: Successful exploitation of this vulnerability will affect availability and confidentiality.	6.2	More Details
CVE-2020-37131	Nsauditor Product Key Explorer 4.2.2.0 contains a denial of service vulnerability that allows local attackers to crash the application by inputting a specially crafted registration key. Attackers can generate a payload of 1000 bytes of repeated characters and paste it into the 'Key' input field to trigger the application crash.	6.2	More Details
CVE-2026-21525	Null pointer dereference in Windows Remote Access Connection Manager allows an unauthorized attacker to deny service locally.	6.2	More Details
CVE-2026-24920	Permission control vulnerability in the AMS module. Impact: Successful exploitation of this vulnerability may affect availability.	6.2	More Details
CVE-2020-37132	UltraVNC Launcher 1.2.4.0 contains a denial of service vulnerability in its password configuration properties that allows local attackers to crash the application. Attackers can paste an overly long 300-character string into the password field to trigger an application crash and prevent normal launcher functionality.	6.2	More Details
CVE-2020-37160	SprintWork 2.3.1 contains multiple local privilege escalation vulnerabilities through insecure file, service, and folder permissions on Windows systems. Local unprivileged users can exploit missing executable files and weak service configurations to create a new administrative user and gain complete system access.	6.2	More Details
CVE-2020-37128	ZOC Terminal 7.25.5 contains a script processing vulnerability that allows local attackers to crash the application by loading a maliciously crafted REXX script file. Attackers can generate an oversized script with 20,000 repeated characters to trigger an application crash and cause a denial of service.	6.2	More Details
CVE-2020-37164	AbsoluteTelnet 11.12 contains a denial of service vulnerability that allows local attackers to crash the application by supplying an oversized license name. Attackers can generate a 2500-character payload and paste it into the license entry field to trigger an application crash.	6.2	More Details
CVE-2020-37171	TapinRadio 2.12.3 contains a denial of service vulnerability in the application proxy username configuration that allows local attackers to crash the application. Attackers can overwrite the username field with 10,000 bytes of arbitrary data to trigger an application crash and prevent normal program functionality.	6.2	More Details
CVE-2020-37165	AbsoluteTelnet 11.12 contains a denial of service vulnerability that allows local attackers to crash the application by supplying an oversized license name. Attackers can generate a 2500-character payload and paste it into the license name field to trigger an application crash.	6.2	More Details
CVE-2020-	TapinRadio 2.12.3 contains a denial of service vulnerability in the application proxy address configuration that allows local attackers to crash the application. Attackers can overwrite the address field with 3000 bytes of arbitrary data to trigger an application crash and	6.2	More Details

37170	prevent normal program functionality.		
CVE-2020-37166	AbsoluteTelnet 11.12 contains a denial of service vulnerability in the SSH2 username input field that allows local attackers to crash the application. Attackers can overwrite the username field with a 1000-byte buffer, causing the application to become unresponsive and terminate.	6.2	More Details
CVE-2026-0946	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal AT Internet SmartTag allows Cross-Site Scripting (XSS).This issue affects AT Internet SmartTag: from 0.0.0 before 1.0.1.	6.1	More Details
CVE-2026-24924	Vulnerability of improper permission control in the print module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	6.1	More Details
CVE-2026-25651	client-certificate-auth is middleware for Node.js implementing client SSL certificate authentication/authorization. Versions 0.2.1 and 0.3.0 of client-certificate-auth contain an open redirect vulnerability. The middleware unconditionally redirects HTTP requests to HTTPS using the unvalidated Host header, allowing an attacker to redirect users to arbitrary domains. This vulnerability is fixed in 1.0.0.	6.1	More Details
CVE-2026-24323	The BSP applications allow an unauthenticated user to inject malicious script content via user-controlled URL parameters that are not sufficiently sanitized. When a victim accesses a crafted URL, the injected script is executed in the victim's browser, leading to a low impact on confidentiality and integrity, and no impact on the availability of the application.	6.1	More Details
CVE-2020-37152	PHP-Fusion 9.03.50 panels.php is vulnerable to cross-site scripting (XSS) via the 'panel_content' POST parameter. The application fails to properly sanitize user input before rendering it in the browser, allowing attackers to inject arbitrary JavaScript. This can be exploited by submitting crafted input to the 'panel_content' field in panels.php, resulting in execution of malicious scripts in the context of the affected site.	6.1	More Details
CVE-2026-2098	AgentFlow developed by Flowring has a Reflected Cross-site Scripting vulnerability, allowing unauthenticated remote attackers to execute arbitrary JavaScript codes in user's browser through phishing attacks.	6.1	More Details
CVE-2026-1643	The MP-Ukagaka plugin for WordPress is vulnerable to Reflected Cross-Site Scripting in all versions up to, and including, 1.5.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2026-24328	SAP TAF_APPLAUNCHER within Business Server Pages allows unauthenticated attacker to craft malicious links that, when clicked by a victim, redirect them to attacker?controlled sites, potentially exposing or altering sensitive information in the victim's browser. This results in a low impact on confidentiality and integrity, with no impact on the availability of the application.	6.1	More Details
CVE-2026-1654	The Peter's Date Countdown plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the `$_SERVER['PHP_SELF']` parameter in all versions up to, and including, 2.0.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2020-37137	PHP-Fusion 9.03.50 contains a remote code execution vulnerability in the 'add_panel_form()' function that allows attackers to execute arbitrary code through an eval() function with unsanitized POST data. Attackers can exploit the vulnerability by sending crafted panel_content POST parameters to the panels.php administration endpoint to execute malicious code.	6.1	More Details
CVE-2026-	The Subitem AL Slider plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the `$_SERVER['PHP_SELF']` parameter in all versions up to, and including, 1.0.0 due to insufficient input sanitization and output escaping. This makes it possible for	6.1	More Details

1634	unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.		
CVE-2026-25516	NiceGUI is a Python-based UI framework. The ui.markdown() component uses the markdown2 library to convert markdown content to HTML, which is then rendered via innerHTML. By default, markdown2 allows raw HTML to pass through unchanged. This means that if an application renders user-controlled content through ui.markdown(), an attacker can inject malicious HTML containing JavaScript event handlers. Unlike other NiceGUI components that render HTML (ui.html(), ui.chat_message(), ui.interactive_image()), the ui.markdown() component does not provide or require a sanitize parameter, leaving applications vulnerable to XSS attacks. This vulnerability is fixed in 3.7.0.	6.1	More Details
CVE-2026-20978	Improper authorization in KnoxGuardManager prior to SMR Feb-2026 Release 1 allows local attackers to bypass the persistence configuration of the application.	6.1	More Details
CVE-2025-70792	Cross Site Scripting vulnerability in the "/admin/category/create" endpoint of Microweber 2.0.19. An attacker can manipulate the "rel_id" parameter in a crafted URL and lure a user with admin privileges into visiting it, achieving JavaScript code execution in the victim's browser. The issue was reported to the developers and fixed in version 2.0.20.	6.1	More Details
CVE-2025-70791	Cross Site Scripting vulnerability in the "/admin/order/abandoned" endpoint of Microweber 2.0.19. An attacker can manipulate the "orderDirection" parameter in a crafted URL and lure a user with admin privileges into visiting it, achieving JavaScript code execution in the victim's browser. The issue was reported to the developers and fixed in version 2.0.20.	6.1	More Details
CVE-2026-0505	The BSP applications allow an unauthenticated user to manipulate user-controlled URL parameters that are not sufficiently validated. This could result in unvalidated redirection to attacker-controlled websites, leading to a low impact on confidentiality and integrity, and no impact on the availability of the application.	6.1	More Details
CVE-2026-25956	Frappe is a full-stack web application framework. Prior to 14.99.14 and 15.94.0, an attacker could craft a malicious signup URL for a frappe site which could lead to an open redirect (or reflected XSS, depending on the crafted payload) when a user signs up. This vulnerability is fixed in 14.99.14 and 15.94.0.	6.1	More Details
CVE-2025-70545	A stored cross-site scripting (XSS) vulnerability exists in the web management interface of the PPC (Belden) ONT 2K05X router running firmware v1.1.9_206L. The Common Gateway Interface (CGI) component improperly handles user-supplied input, allowing a remote, unauthenticated attacker to inject arbitrary JavaScript that is persistently stored and executed when the affected interface is accessed.	6.1	More Details
CVE-2026-25578	Navidrome is an open source web-based music collection server and streamer. Prior to version 0.60.0, a cross-site scripting vulnerability in the frontend allows a malicious attacker to inject code through the comment metadata of a song to exfiltrate user credentials. This issue has been patched in version 0.60.0.	6.1	More Details
CVE-2025-27560	Loop with unreachable exit condition ('infinite loop') for some Intel(R) Platform within Ring 0: Kernel may allow a denial of service. System software adversary with a privileged user combined with a low complexity attack may enable denial of service. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (none), integrity (none) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.0	More Details
CVE-2026-24919	Out-of-bounds write vulnerability in the DFX module. Impact: Successful exploitation of this vulnerability may affect availability.	6.0	More Details
CVE-2026-	Path traversal in ShortcutService prior to SMR Feb-2026 Release 1 allows privileged local attacker to create file with system privilege	6.0	More Details

20982	attacker to create file with system privilege.		Details
CVE-2025-24851	Uncaught exception in the firmware for some 100GbE Intel(R) Ethernet Controller E810 before version cvl fw 1.7.8.x within Ring 0: Bare Metal OS may allow a denial of service. System software adversary with a privileged user combined with a low complexity attack may enable denial of service. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (none), integrity (none) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.0	More Details
CVE-2025-27243	Out-of-bounds write in the firmware for some Intel(R) Ethernet Controller E810 before version cvl fw 1.7.8.x within Ring 0: Bare Metal OS may allow a denial of service. System software adversary with a privileged user combined with a low complexity attack may enable denial of service. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (none), integrity (none) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	6.0	More Details
CVE-2026-1642	A vulnerability exists in NGINX OSS and NGINX Plus when configured to proxy to upstream Transport Layer Security (TLS) servers. An attacker with a man-in-the-middle (MITM) position on the upstream server side—along with conditions beyond the attacker's control—may be able to inject plain text data into the response from an upstream proxied server. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	5.9	More Details
CVE-2025-68686	An Exposure of Sensitive Information to an Unauthorized Actor vulnerability [CWE-200] vulnerability in Fortinet FortiOS 7.6.0 through 7.6.1, FortiOS 7.4.0 through 7.4.6, FortiOS 7.2 all versions, FortiOS 7.0 all versions, FortiOS 6.4 all versions may allow a remote unauthenticated attacker to bypass the patch developed for the symbolic link persistency mechanism observed in some post-exploit cases, via crafted HTTP requests. An attacker would need first to have compromised the product via another vulnerability, at filesystem level.	5.9	More Details
CVE-2026-24931	Vulnerability of improper criterion security check in the card module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	5.9	More Details
CVE-2026-24929	Out-of-bounds read vulnerability in the graphics module. Impact: Successful exploitation of this vulnerability may affect availability.	5.9	More Details
CVE-2026-25518	cert-manager adds certificates and certificate issuers as resource types in Kubernetes clusters, and simplifies the process of obtaining, renewing and using those certificates. In versions from 1.18.0 to before 1.18.5 and from 1.19.0 to before 1.19.3, the cert-manager-controller performs DNS lookups during ACME DNS-01 processing (for zone discovery and propagation self-checks). By default, these lookups use standard unencrypted DNS. An attacker who can intercept and modify DNS traffic from the cert-manager-controller pod can insert a crafted entry into cert-manager's DNS cache. Accessing this entry will trigger a panic, resulting in denial-of-service (DoS) of the cert-manager controller. The issue can also be exploited if the authoritative DNS server for the domain being validated is controlled by a malicious actor. This issue has been patched in versions 1.18.5 and 1.19.3.	5.9	More Details
CVE-2026-24916	Identity authentication bypass vulnerability in the window module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	5.9	More Details
CVE-2026-23684	A race condition vulnerability exists in the SAP Commerce cloud. Because of this when an attacker adds products to a cart, it may result in a cart entry being created with erroneous product value which could be checked out. This leads to high impact on data integrity, with no impact on data confidentiality or availability of the application.	5.9	More Details
	When a BIG-IP Advanced WAF or ASM security policy is configured on a virtual server,		

CVE-2026-22548	undisclosed requests along with conditions beyond the attacker's control can cause the bd process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	5.9	More Details
CVE-2026-25528	LangSmith Client SDKs provide SDK's for interacting with the LangSmith platform. The LangSmith SDK's distributed tracing feature is vulnerable to Server-Side Request Forgery via malicious HTTP headers. An attacker can inject arbitrary api_url values through the baggage header, causing the SDK to exfiltrate sensitive trace data to attacker-controlled endpoints. When using distributed tracing, the SDK parses incoming HTTP headers via RunTree.from_headers() in Python or RunTree.fromHeaders() in Typescript. The baggage header can contain replica configurations including api_url and api_key fields. Prior to the fix, these attacker-controlled values were accepted without validation. When a traced operation completes, the SDK's post() and patch() methods send run data to all configured replica URLs, including any injected by an attacker. This vulnerability is fixed in version 0.6.3 of the Python SDK and 0.4.6 of the JavaScript SDK.	5.8	More Details
CVE-2026-25904	The Pydantic-AI MCP Run Python tool configures the Deno sandbox with an overly permissive configuration that allows the underlying Python code to access the localhost interface of the host to perform SSRF attacks. Note - the "mcp-run-python" project is archived and unlikely to receive a fix.	5.8	More Details
CVE-2026-24319	In SAP Business One, sensitive information is written to the application's memory dump files without obfuscation. Gaining access to this information could potentially lead to unauthorized operations within the B1 environment, including modification of company data. This issue results in a high impact on confidentiality and integrity, with no impact on availability.	5.8	More Details
CVE-2026-25905	The Python code being run by 'runPython' or 'runPythonAsync' is not isolated from the rest of the JS code, allowing any Python code to use the Pyodide APIs to modify the JS environment. This may result in an attacker hijacking the MCP server - for malicious purposes including MCP tool shadowing. Note - the "mcp-run-python" project is archived and unlikely to receive a fix.	5.8	More Details
CVE-2026-24928	Out-of-bounds write vulnerability in the file system module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	5.8	More Details
CVE-2026-25765	Faraday is an HTTP client library abstraction layer that provides a common interface over many adapters. Prior to 2.14.1, Faraday's build_exclusive_url method (in lib/faraday/connection.rb) uses Ruby's URI#merge to combine the connection's base URL with a user-supplied path. Per RFC 3986, protocol-relative URLs (e.g. //evil.com/path) are treated as network-path references that override the base URL's host/authority component. This means that if any application passes user-controlled input to Faraday's get(), post(), build_url(), or other request methods, an attacker can supply a protocol-relative URL like //attacker.com/endpoint to redirect the request to an arbitrary host, enabling Server-Side Request Forgery (SSRF). This vulnerability is fixed in 2.14.1.	5.8	More Details
CVE-2025-55018	An inconsistent interpretation of http requests ('http request smuggling') vulnerability in Fortinet FortiOS 7.6.0, FortiOS 7.4.0 through 7.4.9, FortiOS 7.2 all versions, FortiOS 7.0 all versions, FortiOS 6.4.3 through 6.4.16 may allow an unauthenticated attacker to smuggle an unlogged http request through the firewall policies via a specially crafted header	5.8	More Details
CVE-2026-25870	DoraCMS version 3.1 and prior contains a server-side request forgery (SSRF) vulnerability in its UEditor remote image fetch functionality. The application accepts user-supplied URLs and performs server-side HTTP or HTTPS requests without sufficient validation or destination restrictions. The implementation does not enforce allowlists, block internal or private IP address ranges, or apply request timeouts or response size limits. An attacker can abuse this behavior to induce the server to issue outbound requests to arbitrary hosts, including internal network resources, potentially enabling internal network scanning and denial of service through resource exhaustion.	5.8	More Details
CVE-	The server identity check mechanism for firmware upgrade performed via command shell is insecurely implemented potentially allowing an attacker to perform a Man-in-the-middle		More

2026-22613	attack. This security issue has been fixed in the latest firmware version of Eaton Network M3 which is available on the Eaton download center.	5.7	Details
CVE-2026-21529	Improper neutralization of input during web page generation ('cross-site scripting') in Azure HDInsights allows an authorized attacker to perform spoofing over a network.	5.7	More Details
CVE-2025-12063	An insecure direct object reference allowed a non-admin user to modify or remove certain data objects without having the appropriate permissions.	5.7	More Details
CVE-2026-24885	Kanboard is project management software focused on Kanban methodology. Prior to 1.2.50, a Cross-Site Request Forgery (CSRF) vulnerability exists in the ProjectPermissionController within the Kanboard application. The application fails to strictly enforce the application/json Content-Type for the changeUserRole action. Although the request body is JSON, the server accepts text/plain, allowing an attacker to craft a malicious form using the text/plain attribute. Which allows unauthorized modification of project user roles if an authenticated admin visits a malicious site This vulnerability is fixed in 1.2.50.	5.7	More Details
CVE-2026-25145	melange allows users to build apk packages using declarative pipelines. From version 0.14.0 to before 0.40.3, an attacker who can influence a melange configuration file (e.g., through pull request-driven CI or build-as-a-service scenarios) could read arbitrary files from the host system. The LicensingInfos function in pkg/config/config.go reads license files specified in copyright[].license-path without validating that paths remain within the workspace directory, allowing path traversal via ../ sequences. The contents of the traversed file are embedded into the generated SBOM as license text, enabling exfiltration of sensitive data through build artifacts. This issue has been patched in version 0.40.3.	5.5	More Details
CVE-2026-25920	SumatraPDF is a multi-format reader for Windows. In 3.5.2 and earlier, tA heap out-of-bounds read vulnerability exists in SumatraPDF's MOBI HuffDic decompressor. The bounds check in AddCdicData() only validates half the range that DecodeOne() actually accesses. Opening a crafted .mobi file can read nearly (1 << codeLength) bytes beyond the CDIC dictionary buffer, leading to a crash.	5.5	More Details
CVE-2026-25122	apko allows users to build and publish OCI container images built from apk packages. From version 0.14.8 to before 1.1.0, expandapk.Split drains the first gzip stream of an APK archive via io.Copy(io.Discard, gzi) without explicit bounds. With an attacker-controlled input stream, this can force large gzip inflation work and lead to resource exhaustion (availability impact). The Split function reads the first tar header, then drains the remainder of the gzip stream by reading from the gzip reader directly without any maximum uncompressed byte limit or inflate-ratio cap. A caller that parses attacker-controlled APK streams may be forced to spend excessive CPU time inflating gzip data, leading to timeouts or process slowdown. This issue has been patched in version 1.1.0.	5.5	More Details
CVE-2026-21337	Substance3D - Designer versions 15.1.0 and earlier are affected by an Out-of-bounds Read vulnerability that could lead to memory exposure. An attacker could leverage this vulnerability to access sensitive information stored in memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2025-15314	Tanium addressed an arbitrary file deletion vulnerability in end-user-cx.	5.5	More Details
CVE-2025-15313	Tanium addressed an arbitrary file deletion vulnerability in Tanium EUSS.	5.5	More Details
CVE-2026-21338	Substance3D - Designer versions 15.1.0 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to application denial-of-service. An attacker could exploit this vulnerability to crash the application, causing disruption to services. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
	Substance3D - Designer versions 15.1.0 and earlier are affected by an out-of-bounds read		

CVE-2026-21339	Substance3D - Designer versions 15.1.0 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 stored in memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-21340	Substance3D - Designer versions 15.1.0 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 stored in memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2025-15318	Tanium addressed an arbitrary file deletion vulnerability in End-User Notifications Endpoint Tools.	5.5	More Details
CVE-2026-21358	InDesign Desktop versions 21.1, 20.5.1 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in application denial-of-service. An attacker could exploit this vulnerability to crash the application, causing disruption to services. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-21350	After Effects versions 25.6 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to application denial-of-service. An attacker could exploit this vulnerability to crash the application, causing disruption to services. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-21332	InDesign Desktop versions 21.1, 20.5.1 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 stored in memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-21354	DNG SDK versions 1.7.1 2410 and earlier are affected by an Integer Overflow or Wraparound vulnerability that could lead to application denial-of-service. An attacker could exploit this vulnerability to cause 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-2026-21355	DNG SDK versions 1.7.1 2410 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 stored in memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-21348	Substance3D - Modeler versions 1.22.5 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 stored in memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-20977	Improper access control in Emergency Sharing prior to SMR Feb-2026 Release 1 allows local attackers to interrupt its functioning.	5.5	More Details
CVE-2025-12699	The ZOLL ePCR IOS application reflects unsanitized user input into a WebView. Attacker-controlled strings placed into PCR fields (run number, incident, call sign, notes) are interpreted as HTML/JS when the app prints or renders that content. In the proof of concept (POC), injected scripts return local file content, which would allow arbitrary local file reads from the app's runtime context. These local files contain device and user data within the ePCR medical application, and if exposed, would allow an attacker to access protected health information (PHI) or device telemetry.	5.5	More Details
CVE-2020-37127	Dnsmasq-utils 2.79-1 contains a buffer overflow vulnerability in the dhcp_release utility that allows attackers to cause a denial of service by supplying excessive input. Attackers can trigger a core dump and terminate the dhcp_release process by sending a crafted input string longer than 16 characters.	5.5	More Details
CVE-2026-21336	Substance3D - Designer versions 15.1.0 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to application denial-of-service. An attacker could exploit this vulnerability to crash the application, causing disruption to services. Exploitation	5.5	More Details

	of this issue requires user interaction in that a victim must open a malicious file.		
CVE-2025-15491	The Post Slides WordPress plugin through 1.0.1 does not validate some shortcode attributes before using them to generate paths passed to include function/s, allowing any authenticated users such as with contributor or higher roles to perform LFI attacks	5.5	More Details
CVE-2026-21319	After Effects versions 25.6 and earlier are affected by an Out-of-bounds Read vulnerability that could lead to memory exposure. An attacker could leverage this vulnerability to access sensitive information stored in memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-21261	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to disclose information locally.	5.5	More Details
CVE-2020-37140	Everest, later referred to as AIDA64, 5.50.2100 contains a denial of service vulnerability that allows local attackers to crash the application by manipulating file open functionality. Attackers can generate a 450-byte buffer of repeated characters and paste it into the file open dialog to trigger an application crash.	5.5	More Details
CVE-2026-21317	Audition versions 25.3 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 stored in memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2025-32735	Improper conditions check in some firmware for some Intel(R) NPU Drivers within Ring 1: Device Drivers may allow a denial of service. Unprivileged software adversary with an authenticated user combined with a low complexity attack may enable denial of service. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (none), integrity (none) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	5.5	More Details
CVE-2026-21222	Insertion of sensitive information into log file in Windows Kernel allows an authorized attacker to disclose information locally.	5.5	More Details
CVE-2026-21258	Improper input validation in Microsoft Office Excel allows an unauthorized attacker to disclose information locally.	5.5	More Details
CVE-2020-37121	CODE::BLOCKS 16.01 contains a buffer overflow vulnerability that allows attackers to execute arbitrary code by overwriting Structured Exception Handler with crafted Unicode characters. Attackers can create a malicious M3U playlist file with 536 bytes of buffer and shellcode to trigger remote code execution.	5.5	More Details
CVE-2026-21313	Audition versions 25.3 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 stored in memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-21314	Audition versions 25.3 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 stored in memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-24927	Out-of-bounds access vulnerability in the frequency modulation module. Impact: Successful exploitation of this vulnerability may affect availability.	5.5	More Details
CVE-2026-	Audition versions 25.3 and earlier are affected by an Out-of-bounds Read vulnerability that could lead to memory exposure. An attacker could leverage this vulnerability to access sensitive information stored in memory. Exploitation of this issue requires user interaction in	5.5	More Details

21315	that a victim must open a malicious file.		
CVE-2026-21316	Audition versions 25.3 and earlier are affected by an Access of Memory Location After End of Buffer vulnerability that could lead to application denial-of-service. An attacker could exploit this vulnerability to cause 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-2026-25609	Incorrect validation of the profile command may result in the determination that a request altering the 'filter' is read-only.	5.4	More Details
CVE-2026-2109	A vulnerability was identified in jsbroks COCO Annotator up to 0.11.1. Affected is an unknown function of the file /api/undo/ of the component Delete Category Handler. Such manipulation of the argument ID leads to improper authorization. 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.	5.4	More Details
CVE-2026-25054	n8n is an open source workflow automation platform. Prior to versions 1.123.9 and 2.2.1, a Cross-Site Scripting (XSS) vulnerability existed in a markdown rendering component used in n8n's interface, including workflow sticky notes and other areas that support markdown content. An authenticated user with permission to create or modify workflows could abuse this to execute scripts with same-origin privileges when other users interact with a maliciously crafted workflow. This could lead to session hijacking and account takeover. This issue has been patched in versions 1.123.9 and 2.2.1.	5.4	More Details
CVE-2026-0632	The Fluent Forms Pro Add On Pack plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 6.1.12 via the 'saveDataSource' function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	5.4	More Details
CVE-2025-14895	The PopupKit plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 2.2.0. This is due to the plugin not properly verifying that a user is authorized to access the /popup/logs REST API endpoint. This makes it possible for authenticated attackers, with Subscriber-level access and above, to read and delete analytics data including device types, browser information, countries, referrer URLs, and campaign metrics.	5.4	More Details
CVE-2025-14778	A flaw was found in Keycloak. A significant Broken Access Control vulnerability exists in the UserManagedPermissionService (UMA Protection API). When updating or deleting a UMA policy associated with multiple resources, the authorization check only verifies the caller's ownership against the first resource in the policy's list. This allows a user (Owner A) who owns one resource (RA) to update a shared policy and modify authorization rules for other resources (e.g., RB) in that same policy, even if those other resources are owned by a different user (Owner B). This constitutes a horizontal privilege escalation.	5.4	More Details
CVE-2026-2099	AgentFlow developed by Flowring has a Stored Cross-Site Scripting vulnerability, allowing authenticated remote attackers to inject persistent JavaScript codes that are executed in users' browsers upon page load.	5.4	More Details
CVE-2026-25581	SCEditor is a lightweight WYSIWYG BBCode and XHTML editor. Prior to 3.2.1, if an attacker has the ability control configuration options passed to sceditor.create(), like emoticons, charset, etc. then it's possible for them to trigger an XSS attack due to lack of sanitisation of configuration options. This vulnerability is fixed in 3.2.1.	5.4	More Details
CVE-2026-25574	Payload is a free and open source headless content management system. Prior to 3.74.0, a cross-collection Insecure Direct Object Reference (IDOR) vulnerability exists in the payload-preferences internal collection. In multi-auth collection environments using Postgres or SQLite with default serial/auto-increment IDs, authenticated users from one auth collection can read and delete preferences belonging to users in different auth collections when their numeric IDs collide. This vulnerability has been patched in v3.74.0.	5.4	More Details
	n8n is an open source workflow automation platform. Prior to version 1.123.2, a Cross-Site		

CVE-2026-25051	Scripting (XSS) vulnerability has been identified in the handling of webhook responses and related HTTP endpoints. Under certain conditions, the Content Security Policy (CSP) sandbox protection intended to isolate HTML responses may not be applied correctly. An authenticated user with permission to create or modify workflows could abuse this to execute malicious scripts with same-origin privileges when other users interact with the crafted workflow. This could lead to session hijacking and account takeover. This issue has been patched in version 1.123.2.	5.4	More Details
CVE-2025-68643	Axigen Mail Server before 10.5.57 allows stored Cross-Site Scripting (XSS) in the handling of the timeFormat account preference parameter. Attackers can exploit this by deploying a multi-stage attack. In the first stage, a malicious JavaScript payload is injected into the timeFormat preference by exploiting a separate vulnerability or using compromised credentials. In the second stage, when the victim logs into the WebMail interface, the unsanitized timeFormat value is loaded from storage and inserted into the DOM, causing the injected script to execute.	5.4	More Details
CVE-2026-25889	File Browser provides a file managing interface within a specified directory and it can be used to upload, delete, preview, rename and edit files. Prior to 2.57.1, a case-sensitivity flaw in the password validation logic allows any authenticated user to change their password (or an admin to change any user's password) without providing the current password. By using Title Case field name "Password" instead of lowercase "password" in the API request, the current_password verification is completely bypassed. This enables account takeover if an attacker obtains a valid JWT token through XSS, session hijacking, or other means. This vulnerability is fixed in 2.57.1.	5.4	More Details
CVE-2020-37144	Exagate SYSGuard 6001 contains a cross-site request forgery vulnerability that allows attackers to create unauthorized admin accounts through a crafted HTML form. Attackers can trick users into submitting a malicious form to /kulyon.php that adds a new user with administrative privileges without the victim's consent.	5.3	More Details
CVE-2026-23903	Authentication Bypass by Alternate Name vulnerability in Apache Shiro. This issue affects Apache Shiro: before 2.0.7. Users are recommended to upgrade to version 2.0.7, which fixes the issue. The issue only effects static files. If static files are served from a case-insensitive filesystem, such as default macOS setup, static files may be accessed by varying the case of the filename in the request. If only lower-case (common default) filters are present in Shiro, they may be bypassed this way. Shiro 2.0.7 and later has a new parameters to remediate this issue shiro.ini: filterChainResolver.caseInsensitive = true application.propertie: shiro.caseInsensitive=true Shiro 3.0.0 and later (upcoming) makes this the default.	5.3	More Details
CVE-2025-14831	A flaw was found in GnuTLS. This vulnerability allows a denial of service (DoS) by excessive CPU (Central Processing Unit) and memory consumption via specially crafted malicious certificates containing a large number of name constraints and subject alternative names (SANs).	5.3	More Details
CVE-2026-25523	Magento-lts is a long-term support alternative to Magento Community Edition (CE). Prior to version 20.16.1, the admin url can be discovered without prior knowledge of it's location by exploiting the X-Original-Url header on some configurations. This issue has been patched in version 20.16.1.	5.3	More Details
CVE-2026-0398	Crafted zones can lead to increased resource usage and crafted CNAME chains can lead to cache poisoning in Recursor.	5.3	More Details
CVE-2023-38010	IBM Cloud Pak System displays sensitive information in user messages that could aid in further attacks against the system.	5.3	More Details
CVE-2025-14461	The Xendit Payment plugin for WordPress is vulnerable to unauthorized order status manipulation in all versions up to, and including, 6.0.2. This is due to the plugin exposing a publicly accessible WooCommerce API callback endpoint (`wc_xendit_callback`) that processes payment callbacks without any authentication or cryptographic verification that the requests originate from Xendit's payment gateway. This makes it possible for unauthenticated attackers to mark any WooCommerce order as paid by sending a crafted POST request to the callback URL with a JSON body containing an `external_id` matching	5.3	More Details

	POST request to the callback URL with a JSON body containing an `external_id` matching the order ID pattern and a `status` of 'PAID' or 'SETTLED', granted they can enumerate order IDs (which are sequential integers). This leads to orders being fraudulently marked as completed without any actual payment, resulting in financial loss and inventory depletion.		
CVE-2025-15482	The Chapa Payment Gateway Plugin for WooCommerce plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.0.3 via 'chapa_proceed' WooCommerce API endpoint. This makes it possible for unauthenticated attackers to extract sensitive data including the merchant's Chapa secret API key.	5.3	More Details
CVE-2025-15507	The Magic Import Document Extractor plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the ajax_sync_usage() function in all versions up to, and including, 1.0.4. This makes it possible for unauthenticated attackers to modify the plugin's license status and credit balance.	5.3	More Details
CVE-2025-15508	The Magic Import Document Extractor plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.0.4 via the get_frontend_settings() function. This makes it possible for unauthenticated attackers to extract the site's magicimport.ai license key from the page source on any page containing the plugin's shortcode.	5.3	More Details
CVE-2026-0679	The Fortis for WooCommerce plugin for WordPress is vulnerable to authorization bypass due to an inverted nonce check in the 'check_fortis_notify_response' function in all versions up to, and including, 1.2.0. This makes it possible for unauthenticated attackers to update arbitrary WooCommerce order statuses to paid/processing/completed, effectively allowing them to mark orders as paid without payment.	5.3	More Details
CVE-2025-31944	Race condition for some TDX Module before version tdx1.5 within Ring 0: Hypervisor may allow a denial of service. Authorized adversary with a privileged user combined with a high complexity attack may enable denial of service. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (none), integrity (none) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (low) impacts.	5.3	More Details
CVE-2025-27535	Exposed ioctl with insufficient access control in the firmware for some Intel(R) Ethernet Connection E825-C. before version NVM ver. 3.84 within Ring 0: Bare Metal OS may allow a denial of service. System software adversary with a privileged user combined with a high complexity attack may enable denial of service. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (none), integrity (none) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	5.3	More Details
CVE-2025-15570	A vulnerability was found in ckolivas lrzip up to 0.651. This impacts the function lzma_decompress_buf of the file stream.c. Performing a manipulation results in use after free. Attacking locally is a requirement. The exploit has been made public and could be used. The project was informed of the problem early through an issue report but has not responded yet.	5.3	More Details
CVE-2026-23623	Collabora Online is a collaborative online office suite based on LibreOffice technology. Prior to Collabora Online Development Edition version 25.04.08.2 and prior to Collabora Online versions 23.05.20.1, 24.04.17.3, and 25.04.7.5, a user with view-only rights and no download privileges can obtain a local copy of a shared file. Although there are no corresponding buttons in the interface, pressing Ctrl+Shift+S initiates the file download process. This allows the user to bypass the access restrictions and leads to unauthorized data retrieval. This issue has been patched in Collabora Online Development Edition version 25.04.08.2 and Collabora Online versions 23.05.20.1, 24.04.17.3, and 25.04.7.5.	5.3	More Details
CVE-2026-24027	Crafted zones can lead to increased incoming network traffic.	5.3	More Details
CVE-	A vulnerability has been identified in syngo.plaza VB30E (All versions < VB30E_HF07). The		More

2024-52334	affected application does not encrypt the passwords properly. This could allow an attacker to recover the original passwords and might gain unauthorized access.	5.3	Details
CVE-2026-1722	The WCFM Marketplace – Multivendor Marketplace for WooCommerce plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 3.7.0. This is due to the plugin not implementing authorization checks in the `wcfm-refund-requests-form` AJAX controller. This makes it possible for unauthenticated attackers to create arbitrary refund requests for any order ID and item ID, potentially leading to financial loss if automatic refund approval is enabled in the plugin settings.	5.3	More Details
CVE-2023-38281	IBM Cloud Pak System does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic.	5.3	More Details
CVE-2024-39724	IBM Db2 Big SQL on Cloud Pak for Data versions 7.6 (on CP4D 4.8), 7.7 (on CP4D 5.0), and 7.8 (on CP4D 5.1) do not properly limit the allocation of system resources. An authenticated user with internal knowledge of the environment could exploit this weakness to cause a denial of service.	5.3	More Details
CVE-2026-0944	Improper Check for Unusual or Exceptional Conditions vulnerability in Drupal Group invite allows Forceful Browsing.This issue affects Group invite: from 0.0.0 before 2.3.9, from 3.0.0 before 3.0.4, from 4.0.0 before 4.0.4.	5.3	More Details
CVE-2026-24321	SAP Commerce Cloud exposes multiple API endpoints to unauthenticated users, allowing them to submit requests to these open endpoints to retrieve sensitive information that is not intended to be publicly accessible via the front-end. This vulnerability has a low impact on confidentiality and does not affect integrity and availability.	5.3	More Details
CVE-2025-14079	The ELEX WordPress HelpDesk & Customer Ticketing System plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 3.3.5. This is due to missing capability checks on the eh_crm_ticket_general function combined with a shared nonce that is exposed to low-privileged users. This makes it possible for authenticated attackers, with Subscriber-level access and above, to modify global WSDesk settings via the `eh_crm_ticket_general` AJAX action.	5.3	More Details
CVE-2026-1271	The ProfileGrid – User Profiles, Groups and Communities plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 5.9.7.2 via the 'pm_upload_image' and 'pm_upload_cover_image' AJAX actions. This is due to the update_user_meta() function being called outside of the user authorization check in public/partials/crop.php and public/partials/coverimg_crop.php. This makes it possible for authenticated attackers, with Subscriber-level access and above, to change any user's profile picture or cover image, including administrators.	5.3	More Details
CVE-2023-38017	IBM Cloud Pak System is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	5.3	More Details
CVE-2026-25872	JUNG Smart Panel KNX firmware version L1.12.22 and prior contain an unauthenticated path traversal vulnerability in the embedded web interface. The application fails to properly validate file path input, allowing remote, unauthenticated attackers to access arbitrary files on the underlying filesystem within the context of the web server. This may result in disclosure of system configuration files and other sensitive information.	5.3	More Details
CVE-2026-2062	A vulnerability was identified in Open5GS up to 2.7.6. This affects the function sgwc_s5c_handle_modify_bearer_response/sgwc_sxa_handle_session_modification_response of the component PGW S5U Address Handler. The manipulation leads to null pointer dereference. The attack can be initiated remotely. The exploit is publicly available and might be used. The identifier of the patch is f1bbd7b57f831e2a070780a7d8d5d4c73babdb59. Applying a patch is the recommended action to fix this issue.	5.3	More Details
CVE-	A vulnerability was detected in kalyan02 NanoCMS up to 0.4. Affected by this issue is some unknown functionality of the file /data/pagesdata.txt of the component User Information		

2026-1978	Handler. Performing a manipulation results in direct request. It is possible to initiate the attack remotely. The exploit is now public and may be used. You should change the configuration settings.	5.3	More Details
CVE-2026-1675	The Advanced Country Blocker plugin for WordPress is vulnerable to Authorization Bypass in all versions up to, and including, 2.3.1 due to the use of a predictable default value for the secret bypass key created during installation without requiring users to change it. This makes it possible for unauthenticated attackers to bypass the geolocation blocking mechanism by appending the key to any URL on sites where the administrator has not changed the default value.	5.3	More Details
CVE-2026-2207	A weakness has been identified in WeKan up to 8.20. This issue affects some unknown processing of the file server/publications/activities.js of the component Activity Publication Handler. Executing a manipulation can lead to information disclosure. It is possible to launch the attack remotely. Upgrading to version 8.21 is capable of addressing this issue. This patch is called 91a936e07d2976d4246dfe834281c3aaa87f9503. You should upgrade the affected component.	5.3	More Details
CVE-2025-10753	The OAuth Single Sign On – SSO (OAuth Client) plugin for WordPress is vulnerable to unauthorized access in all versions up to, and including, 6.26.14. This is due to missing capability checks and authentication verification on the OAuth redirect functionality accessible via the 'oauthredirect' option parameter. This makes it possible for unauthenticated attackers to set the global redirect URL option via the redirect_url parameter granted they can access the site directly.	5.3	More Details
CVE-2020-37106	Business Live Chat Software 1.0 contains a cross-site request forgery vulnerability that allows attackers to change user account roles without authentication. Attackers can craft a malicious HTML form to modify user privileges by submitting a POST request to the user creation endpoint with administrative access parameters.	5.3	More Details
CVE-2026-25123	Homarr is an open-source dashboard. Prior to 1.52.0, a public (unauthenticated) tRPC endpoint widget.app.ping accepts an arbitrary url and performs a server-side request to that URL. This allows an unauthenticated attacker to trigger outbound HTTP requests from the Homarr server, enabling SSRF behavior and a reliable port-scanning primitive (open vs closed ports can be inferred from statusCode vs fetch failed and timing). This vulnerability is fixed in 1.52.0.	5.3	More Details
CVE-2026-2016	A security vulnerability has been detected in happyfish100 libfastcommon up to 1.0.84. Affected by this vulnerability is the function base64_decode of the file src/base64.c. The manipulation leads to stack-based buffer overflow. Local access is required to approach this attack. The exploit has been disclosed publicly and may be used. The identifier of the patch is 82f66af3e252e3e137dba0c3891570f085e79adf. Applying a patch is the recommended action to fix this issue.	5.3	More Details
CVE-2026-1973	A vulnerability was determined in Free5GC up to 4.1.0. The impacted element is the function establishPfcpSession of the component SMF. Executing a manipulation can lead to null pointer dereference. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized. It is best practice to apply a patch to resolve this issue.	5.3	More Details
CVE-2026-2147	A weakness has been identified in Tenda AC21 16.03.08.16. This impacts an unknown function of the file /cgi-bin/DownloadLog of the component Web Management Interface. Executing a manipulation can lead to information disclosure. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks.	5.3	More Details
CVE-2026-1975	A security flaw has been discovered in Free5GC up to 4.1.0. This impacts the function identityTriggerType of the file pfcp_reports.go. The manipulation results in null pointer dereference. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks. Applying a patch is advised to resolve this issue.	5.3	More Details
CVE-	PrestaShop is an open source e-commerce web application. Prior to 8.2.4 and 9.0.3, there is a time-based user enumeration vulnerability in the user authentication functionality of		

CVE-2026-25597	a time-based user enumeration vulnerability in the user authentication functionality of PrestaShop. This vulnerability allows an attacker to determine whether a customer account exists in the system by measuring response times. This vulnerability is fixed in 8.2.4 and 9.0.3.	5.3	More Details
CVE-2026-1974	A vulnerability was identified in Free5GC up to 4.1.0. This affects the function ResolveNodeIdToIp of the file internal/sbi/processor/datapath.go of the component SMF. The manipulation leads to denial of service. Remote exploitation of the attack is possible. The exploit is publicly available and might be used. It is recommended to apply a patch to fix this issue.	5.3	More Details
CVE-2026-2108	A vulnerability was determined in jsbroks COCO Annotator up to 0.11.1. This impacts an unknown function of the file /api/info/long_task of the component Endpoint. This manipulation causes denial of service. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2026-2148	A security vulnerability has been detected in Tenda AC21 16.03.08.16. Affected is an unknown function of the file /cgi-bin/DownloadFlash of the component Web Management Interface. The manipulation leads to information disclosure. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used.	5.3	More Details
CVE-2026-1976	A weakness has been identified in Free5GC up to 4.1.0. Affected is the function SessionDeletionResponse of the component SMF. This manipulation causes null pointer dereference. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks. It is suggested to install a patch to address this issue.	5.3	More Details
CVE-2026-2056	A security vulnerability has been detected in D-Link DIR-605L and DIR-619L 2.06B01/2.13B01. The impacted element is an unknown function of the file /wan_connection_status.asp of the component DHCP Connection Status Handler. The manipulation leads to information disclosure. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	5.3	More Details
CVE-2026-1972	A vulnerability was found in Edimax BR-6208AC 2_1.02. The affected element is the function auth_check_userpass2. Performing a manipulation of the argument Username/Password results in use of default credentials. The attack may be initiated remotely. The exploit has been made public and could be used. The vendor confirms that the affected product is end-of-life. They confirm that they "will issue a consolidated Security Advisory on our official support website." This vulnerability only affects products that are no longer supported by the maintainer.	5.3	More Details
CVE-2026-2055	A weakness has been identified in D-Link DIR-605L and DIR-619L 2.06B01/2.13B01. The affected element is an unknown function of the component DHCP Client Information Handler. Executing a manipulation can lead to information disclosure. The attack may be launched remotely. The exploit has been made available to the public and could be used for attacks. This vulnerability only affects products that are no longer supported by the maintainer.	5.3	More Details
CVE-2026-1769	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Xerox CentreWare on Windows allows Stored XSS.This issue affects CentreWare: through 7.0.6. Consider upgrading Xerox® CentreWare Web® to v7.2.2.25 via the software available on Xerox.com	5.3	More Details
CVE-2026-2054	A security flaw has been discovered in D-Link DIR-605L and DIR-619L 2.06B01/2.13B01. Impacted is an unknown function of the component Wifi Setting Handler. Performing a manipulation results in information disclosure. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks. This vulnerability only affects products that are no longer supported by the maintainer.	5.3	More Details
CVE-2026-	A flaw has been found in mruby up to 3.4.0. This affects the function mrb_vm_exec of the file src/vm.c of the component JMPNOT-to-JMPIF Optimization. Executing a manipulation can lead to use after free. The attack needs to be launched locally. The exploit has been	5.3	More

1979	published and may be used. This patch is called e50f15c1c6e131fa7934355eb02b8173b13df415. It is advisable to implement a patch to correct this issue.		Details
CVE-2026-24312	An erroneous authorization check in SAP Business Workflow leads to privilege escalation. An authenticated administrative user can bypass role restrictions by leveraging permissions from a less sensitive function to execute unauthorized, high-privilege actions. This has a high impact on data integrity, with low impact on confidentiality and no impact on availability of the application.	5.2	More Details
CVE-2025-13491	IBM App Connect Enterprise Certified Container up to 12.19.0 (Continuous Delivery) and 12.0 LTS (Long Term Support) could allow an attacker to access sensitive files or modify configurations due to an untrusted search path.	5.1	More Details
CVE-2025-69619	A path traversal in My Text Editor v1.6.2 allows attackers to cause a Denial of Service (DoS) via writing files to the internal storage.	5.0	More Details
CVE-2026-1892	A security vulnerability has been detected in WeKan up to 8.20. This affects the function setBoardOrgs of the file models/boards.js of the component REST API. Such manipulation of the argument item.cardId/item.checklistId/card.boardId leads to improper authorization. The attack may be launched remotely. A high complexity level is associated with this attack. The exploitability is reported as difficult. Upgrading to version 8.21 mitigates this issue. The name of the patch is cabfeed9a68e21c469bf206d8655941444b9912c. It is suggested to upgrade the affected component.	5.0	More Details
CVE-2025-11537	A flaw was found in Keycloak. When the logging format is configured to a verbose, user-supplied pattern (such as the pre-defined 'long' pattern), sensitive headers including Authorization and Cookie are disclosed to the logs in cleartext. An attacker with read access to the log files can extract these credentials (e.g., bearer tokens, session cookies) and use them to impersonate users, leading to a full account compromise.	5.0	More Details
CVE-2026-0486	In ABAP based SAP systems a remote enabled function module does not perform necessary authorization checks for an authenticated user resulting in disclosure of system information.This has low impact on confidentiality. Integrity and availability are not impacted.	5.0	More Details
CVE-2025-70347	An issue in mquickjs before commit 74b7e (2026-01-15) allows a local attacker to cause a denial of service via a crafted file to the get_mblock_size function at mquickjs.c.	5.0	More Details
CVE-2024-54192	An issue inTcpreplay v4.5.1 allows a local attacker to cause a denial of service via a crafted file to the tcpedit_dlt_getplugin function at src/tcpedit/plugins/dlt_utils.c.	5.0	More Details
CVE-2025-69620	A path traversal in Moo Chan Song v4.5.7 allows attackers to cause a Denial of Service (DoS) via writing files to the internal storage.	5.0	More Details
CVE-2025-15328	Tanium addressed an improper link resolution before file access vulnerability in Enforce.	5.0	More Details
CVE-2026-22549	A vulnerability exists in F5 BIG-IP Container Ingress Services that may allow excessive permissions to read cluster secrets. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	4.9	More Details
CVE-2026-1370	The SIBS woocommerce payment gateway plugin for WordPress is vulnerable to time-based SQL Injection via the ‘referencedId’ parameter in all versions up to, and including, 2.2.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	4.9	More Details

CVE-2025-15332	Tanium addressed an information disclosure vulnerability in Threat Response.	4.9	More Details
CVE-2025-15329	Tanium addressed an information disclosure vulnerability in Threat Response.	4.9	More Details
CVE-2025-15487	The Code Explorer plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 1.4.6 via the 'file' parameter. This makes it possible for authenticated attackers, with Administrator-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information.	4.9	More Details
CVE-2026-1246	The ShortPixel Image Optimizer plugin for WordPress is vulnerable to Arbitrary File Read via path traversal in the 'loadFile' parameter in all versions up to, and including, 6.4.2 due to insufficient path validation and sanitization in the 'loadLogFile' AJAX action. This makes it possible for authenticated attackers, with Editor-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information such as database credentials and authentication keys.	4.9	More Details
CVE-2026-0816	The All push notification for WP plugin for WordPress is vulnerable to time-based SQL Injection via the 'delete_id' parameter in all versions up to, and including, 1.5.3 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	4.9	More Details
CVE-2026-1553	Incorrect Authorization vulnerability in Drupal Drupal Canvas allows Forceful Browsing.This issue affects Drupal Canvas: from 0.0.0 before 1.0.4.	4.8	More Details
CVE-2026-24325	SAP BusinessObjects Enterprise does not sufficiently encode user-controlled inputs, leading to Stored Cross-Site Scripting (XSS) vulnerability. This enables an admin user to inject malicious JavaScript into a website and the injected script gets executed when the user visits the compromised page.This vulnerability has low impact on confidentiality and integrity of the data. There is no impact on the availability of the application.	4.8	More Details
CVE-2026-0947	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal AT Internet Piano Analytics allows Cross-Site Scripting (XSS).This issue affects AT Internet Piano Analytics: from 0.0.0 before 1.0.1, from 2.0.0 before 2.3.1.	4.8	More Details
CVE-2026-24921	Address read vulnerability in the HDC module. Impact: Successful exploitation of this vulnerability will affect availability and confidentiality.	4.8	More Details
CVE-2026-20111	A vulnerability in the web-based management interface of Cisco Prime Infrastructure could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against users of the interface of an affected system. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by inserting malicious code into specific data fields in the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, an attacker must have valid administrative credentials.	4.8	More Details
CVE-2026-2000	A vulnerability was found in DCN DCME-320 up to 20260121. Impacted is the function apply_config of the file /function/system/basic/bridge_cfg.php of the component Web Management Backend. Performing a manipulation of the argument ip_list results in command injection. The attack is possible to be carried out remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2026-	A security vulnerability has been detected in PHPGurukul Hospital Management System 4.0. The affected element is an unknown function of the file /hms/admin/manage-doctors.php.	4.7	More

2026-2134	Such manipulation of the argument ID leads to sql injection. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.	4.7	Details
CVE-2026-2063	A security flaw has been discovered in D-Link DIR-823X 250416. This vulnerability affects unknown code of the file /goform/set_ac_server of the component Web Management Interface. The manipulation of the argument ac_server results in os command injection. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks.	4.7	More Details
CVE-2026-2081	A vulnerability was determined in D-Link DIR-823X 250416. The affected element is an unknown function of the file /goform/set_password. This manipulation of the argument http_passwd causes os command injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	4.7	More Details
CVE-2026-2163	A vulnerability was identified in D-Link DIR-600 up to 2.15WWb02. This vulnerability affects unknown code of the file ssdp.cgi. Such manipulation of the argument HTTP_ST/REMOTE_ADDR/REMOTE_PORT/SERVER_ID leads to command injection. The attack may be launched remotely. The exploit is publicly available and might be used. This vulnerability only affects products that are no longer supported by the maintainer.	4.7	More Details
CVE-2026-2213	A security flaw has been discovered in code-projects Online Music Site 1.0. Affected by this issue is some unknown functionality of the file /Administrator/PHP/AdminAddAlbum.php. The manipulation of the argument txtimage results in unrestricted upload. The attack may be performed from remote. The exploit has been released to the public and may be used for attacks.	4.7	More Details
CVE-2026-1884	A weakness has been identified in ZenTao up to 21.7.6-85642. The impacted element is the function fetchHook of the file module/webhook/model.php of the component Webhook Module. This manipulation causes server-side request forgery. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2025-35992	Improper conditions check in some firmware for some Intel(R) NPU Drivers within Ring 1: Device Drivers may allow a denial of service. Unprivileged software adversary with an authenticated user combined with a high complexity attack may enable denial of service. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (none), integrity (none) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	4.7	More Details
CVE-2026-2226	A vulnerability has been found in DouPHP up to 1.9. This issue affects some unknown processing of the file /admin/file.php of the component ZIP File Handler. Such manipulation of the argument sql_filename leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	4.7	More Details
CVE-2026-2227	A vulnerability was found in D-Link DCS-931L up to 1.13.0. Impacted is the function doSystem of the file /setSystemAdmin. Performing a manipulation of the argument AdminID results in command injection. The attack may be initiated remotely. The exploit has been made public and could be used. This vulnerability only affects products that are no longer supported by the maintainer.	4.7	More Details
CVE-2026-2162	A vulnerability was determined in itsourcecode News Portal Project 1.0. This affects an unknown part of the file /admin/aboutus.php. This manipulation of the argument pagetitle causes sql injection. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized.	4.7	More Details
CVE-2025-22885	Improper buffer restrictions in the firmware for the TDX Module may allow an escalation of privilege. System software adversary with a privileged user combined with a high complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (high), integrity (low) and availability (none) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	4.7	More Details

CVE-2026-1517	A vulnerability was identified in iomad up to 5.0. Affected is an unknown function of the component Company Admin Block. Such manipulation leads to sql injection. The attack can be executed remotely. It is best practice to apply a patch to resolve this issue.	4.7	More Details
CVE-2026-2082	A vulnerability was identified in D-Link DIR-823X 250416. The impacted element is an unknown function of the file /goform/set_mac_clone. Such manipulation of the argument mac leads to os command injection. The attack may be performed from remote. The exploit is publicly available and might be used.	4.7	More Details
CVE-2026-2179	A vulnerability was determined in PHPGurukul Hospital Management System 4.0. This impacts an unknown function of the file /admin/manage-users.php. This manipulation of the argument ID causes sql injection. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized.	4.7	More Details
CVE-2026-2061	A vulnerability was determined in D-Link DIR-823X 250416. Affected by this issue is the function sub_424D20 of the file /goform/set_ipv6. Executing a manipulation can lead to os command injection. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized.	4.7	More Details
CVE-2025-63354	Hitron HI3120 v7.2.4.5.2b1 allows stored XSS via the Parental Control option when creating a new filter. The device fails to properly handle inputs, allowing an attacker to inject and execute JavaScript.	4.6	More Details
CVE-2026-25230	FileRise is a self-hosted web file manager / WebDAV server. Prior to 3.3.0, an HTML Injection vulnerability allows an authenticated user to modify the DOM and add e.g. form elements that call certain endpoints or link elements that redirect the user on active interaction. This vulnerability is fixed in 3.3.0.	4.6	More Details
CVE-2026-1763	Vulnerability in GE Vernova Enervista UR Setup on Windows.This issue affects Enervista: 8.6 and previous versions.	4.6	More Details
CVE-2025-12757	An AXIS Camera Station Pro feature can be exploited in a way that allows a non-admin user to view information they are not permitted to.	4.6	More Details
CVE-2026-25647	Lute is a structured Markdown engine supporting Go and JavaScript. Lute 1.7.6 and earlier (as used in SiYuan before) has a Stored Cross-Site Scripting (XSS) vulnerability in the Markdown rendering engine. An attacker can inject malicious JavaScript into a Markdown text/note. When another user clicks the rendered content, the script executes in the context of their session.	4.6	More Details
CVE-2025-13064	A server-side injection was possible for a malicious admin to manipulate the application to include a malicious script which is executed by the server. This attack is only possible if the admin uses a client that have been tampered with.	4.5	More Details
CVE-2025-32007	Out-of-bounds read for some TDX before version tdx module 1.5.24 within Ring 0: Hypervisor may allow an information disclosure. Authorized adversary with a privileged user combined with a low complexity attack may enable data exposure. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (high), integrity (none) and availability (none) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	4.4	More Details
CVE-2026-23685	Due to a Deserialization vulnerability in SAP NetWeaver (JMS service), an attacker authenticated as an administrator with local access could submit specially crafted content to the server. If processed by the application, this content could trigger unintended behavior during internal logic execution, potentially causing a denial of service. Successful exploitation results in a high impact on availability, while confidentiality and integrity remain unaffected.	4.4	More Details
	The Extended Random Number Generator plugin for WordPress is vulnerable to Stored		

CVE-2026-0681	Cross-Site Scripting via the plugin settings in all versions up to, and including, 1.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2026-0743	The WP Content Permission plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'ohmem-message' parameter in all versions up to, and including, 1.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	4.4	More Details
CVE-2026-25567	WeKan versions prior to 8.19 contain an insecure direct object reference (IDOR) in the card comment creation API. The endpoint accepts an authorId from the request body, allowing an authenticated user to spoof the recorded comment author by supplying another user's identifier.	4.3	More Details
CVE-2026-24327	Due to missing authorization check in SAP Strategic Enterprise Management (Balanced Scorecard in Business Server Pages), an authenticated attacker could access information that they are otherwise unauthorized to view. This leads to low impact on confidentiality and no effect on integrity or availability.	4.3	More Details
CVE-2026-1082	The TITLE ANIMATOR plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0. This is due to missing nonce validation on the settings page form handler in `inc/settings-page.php`. This makes it possible for unauthenticated attackers to modify plugin settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2026-25642	HedgeDoc is an open source, real-time, collaborative, markdown notes application. Prior to 1.10.6, files served below the /uploads/ endpoint did not use a more strict security-policy. This resulted in a too open Content-Security-Policy and furthermore opened the possibility to host malicious interactive web content (such as fake login forms) using SVG files. This vulnerability is fixed in 1.10.6.	4.3	More Details
CVE-2026-25568	WeKan versions prior to 8.19 contain an authorization logic vulnerability where the instance configuration setting allowPrivateOnly is not sufficiently enforced at board creation time. When allowPrivateOnly is enabled, users can still create public boards due to incomplete server-side enforcement.	4.3	More Details
CVE-2025-13416	The ProfileGrid – User Profiles, Groups and Communities plugin for WordPress is vulnerable to unauthorized user suspension due to a missing capability check on the pm_deactivate_user_from_group() function in all versions up to, and including, 5.9.7.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to suspend arbitrary users from groups, including administrators, via the pm_deactivate_user_from_group AJAX action.	4.3	More Details
CVE-2026-2111	A weakness has been identified in JeecgBoot up to 3.9.0. Affected by this issue is some unknown functionality of the file /airag/knowledge/doc/edit of the component Retrieval-Augmented Generation Module. Executing a manipulation of the argument filePath can lead to path traversal. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2026-2149	A vulnerability was detected in SourceCodester/Patrick Mvuma Patients Waiting Area Queue Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /appointments.php. The manipulation of the argument patient_id results in cross site scripting. It is possible to launch the attack remotely. The exploit is now public and may be used.	4.3	More Details
CVE-2026-2150	A flaw has been found in SourceCodester/Patrick Mvuma Patients Waiting Area Queue Management System 1.0. Affected by this issue is some unknown functionality of the file /checkin.php. This manipulation of the argument patient_id causes cross site scripting. The attack can be initiated remotely. The exploit has been published and may be used.	4.3	More Details

CVE-2026-24326	Due to a missing authorization check in the Disconnected Operations of the SAP S/4HANA Defense & Security, an attacker with user privileges could call remote-enabled function modules to do direct update on standard SAP database table . This results in low impact on integrity, with no impact on confidentiality or availability of the application.	4.3	More Details
CVE-2026-23688	SAP Fiori App Manage Service Entry Sheets does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. This has low impact on integrity, confidentiality and availability are not impacted.	4.3	More Details
CVE-2026-20123	A vulnerability in the web-based management interface of Cisco Evolved Programmable Network Manager (EPNM) and Cisco Prime Infrastructure could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in the HTTP request. An attacker could exploit this vulnerability by intercepting and modifying an HTTP request from a user. A successful exploit could allow the attacker to redirect the user to a malicious web page.	4.3	More Details
CVE-2026-1897	A vulnerability was found in WeKan up to 8.20. Affected by this issue is some unknown functionality of the file server/methods/positionHistory.js of the component Position-History Tracking. The manipulation results in missing authorization. The attack may be performed from remote. Upgrading to version 8.21 can resolve this issue. The patch is identified as 55576ec17722db094835470b386162c9a662fb60. It is advisable to upgrade the affected component.	4.3	More Details
CVE-2026-23681	Due to missing authorization check in a function module in SAP Support Tools Plug-In, an authenticated attacker could invoke specific function modules to retrieve information about the system and its configuration. This disclosure of the system information could assist the attacker to plan subsequent attacks. This vulnerability has a low impact on the confidentiality of the application, with no effect on its integrity or availability.	4.3	More Details
CVE-2026-2205	A vulnerability was identified in WeKan up to 8.20. This affects an unknown part of the file server/publications/cards.js of the component Meteor Publication Handler. Such manipulation leads to information disclosure. The attack may be performed from remote. Upgrading to version 8.21 is able to mitigate this issue. The name of the patch is 0f5a9c38778ca550cbab6c5093470e1e90cb837f. Upgrading the affected component is advised.	4.3	More Details
CVE-2026-24776	OpenProject is an open-source, web-based project management software. Prior to 17.0.2, the drag&drop handler moving an agenda item to a different section was not properly checking if the target meeting section is part of the same meeting (or is the backlog, in case of recurring meetings). This allowed an attacker to move a meeting agenda item into a different meeting. The attacker did not get access to meetings, but they could add arbitrary agenda items, that could cause confusions. The vulnerability is fixed in 17.0.2.	4.3	More Details
CVE-2024-40685	IBM Operations Analytics – Log Analysis versions 1.3.5.0 through 1.3.8.3 and IBM SmartCloud Analytics – Log Analysis are vulnerable to a cross-site request forgery (CSRF) vulnerability that could allow an attacker to trick a trusted user into performing unauthorized actions.	4.3	More Details
CVE-2026-2208	A security vulnerability has been detected in WeKan up to 8.20. Impacted is an unknown function of the file server/publications/rules.js of the component Rules Handler. The manipulation leads to missing authorization. The attack can be initiated remotely. Upgrading to version 8.21 is recommended to address this issue. The identifier of the patch is a787bcddf33ca28afb13ff5ea9a4cb92dceac005. The affected component should be upgraded.	4.3	More Details
CVE-2025-15147	The WCFM Membership – WooCommerce Memberships for Multivendor Marketplace plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 2.11.8 via the 'WCFMvm_Memberships_Payment_Controller::processing' due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Subscriber-level access and above, to modify other users' membership payments.	4.3	More Details
	go-git is a highly extensible git implementation library written in pure Go. Prior to 5.16.5, a		

CVE-2026-25934	vulnerability was discovered in go-git whereby data integrity values for .pack and .idx files were not properly verified. This resulted in go-git potentially consuming corrupted files, which would likely result in unexpected errors such as object not found. For context, clients fetch packfiles from upstream Git servers. Those files contain a checksum of their contents, so that clients can perform integrity checks before consuming it. The pack indexes (.idx) are generated locally by go-git, or the git cli, when new .pack files are received and processed. The integrity checks for both files were not being verified correctly. This vulnerability is fixed in 5.16.5.	4.3	More Details
CVE-2026-23624	GLPI is a free asset and IT management software package. In versions starting from 0.71 to before 10.0.23 and before 11.0.5, when remote authentication is used, based on SSO variables, a user can steal a GLPI session previously opened by another user on the same machine. This issue has been patched in versions .	4.3	More Details
CVE-2025-15476	The The Bucketlister plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the bucketlister_do_admin_ajax() function in all versions up to, and including, 0.1.5. This makes it possible for authenticated attackers, with Subscriber-level access and above, to add delete or modify arbitrary bucket list items.	4.3	More Details
CVE-2026-1835	A vulnerability was identified in lcg0124 BootDo up to e93dd428ef6f5c881aa74d49a2099ab0cf1e0fcb. This affects an unknown part. The manipulation leads to cross-site request forgery. The attack is possible to be carried out remotely. The exploit is publicly available and might be used. This product adopts a rolling release strategy to maintain continuous delivery. Therefore, version details for affected or updated releases cannot be specified.	4.3	More Details
CVE-2026-1785	The Code Snippets plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.9.4. This is due to missing nonce validation on the cloud snippet download and update actions in the Cloud_Search_List_Table class. This makes it possible for unauthenticated attackers to force logged-in administrators to download or update cloud snippets without their consent via a crafted request, granted they can trick an administrator into visiting a malicious page.	4.3	More Details
CVE-2026-25562	WeKan versions prior to 8.19 contain an information disclosure vulnerability in the attachments publication. Attachment metadata can be returned without properly scoping results to boards and cards accessible to the requesting user, potentially exposing attachment metadata to unauthorized users.	4.3	More Details
CVE-2025-15327	Tanium addressed an improper access controls vulnerability in Deploy.	4.3	More Details
CVE-2025-15334	Tanium addressed an information disclosure vulnerability in Threat Response.	4.3	More Details
CVE-2026-25530	Kanboard is project management software focused on Kanban methodology. Prior to 1.2.50, the getSwimlane API method lacks project-level authorization, allowing authenticated users to access swimlane data from projects they cannot access. This vulnerability is fixed in 1.2.50.	4.3	More Details
CVE-2025-15326	Tanium addressed an improper access controls vulnerability in Patch.	4.3	More Details
CVE-2026-2159	A flaw has been found in SourceCodester Simple Responsive Tourism Website 1.0. Affected is an unknown function of the file /tourism/classes/Master.php?f=register of the component Registration. Executing a manipulation of the argument firstname/lastname/username can lead to cross site scripting. It is possible to launch the attack remotely. The exploit has been published and may be used.	4.3	More Details
CVE-	The Timeline Block – Beautiful Timeline Builder for WordPress (Vertical & Horizontal Timelines) plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 1.3.3 via the tlgb_shortcode() function due to missing		More

2026-1228	versions up to, and including, 1.5.5 via the tlgb_shortcode() function due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Author-level access and above, to disclose private timeline content via the id attribute supplied to the 'timeline_block' shortcode.	4.3	More Details
CVE-2025-15331	Tanium addressed an uncontrolled resource consumption vulnerability in Connect.	4.3	More Details
CVE-2026-2154	A vulnerability was identified in SourceCodester/Patrick Mvuma Patients Waiting Area Queue Management System 1.0. Impacted is an unknown function of the file /registration.php of the component Patient Registration Module. The manipulation of the argument First Name leads to cross site scripting. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.	4.3	More Details
CVE-2026-2153	A vulnerability was determined in mwielgoszewski doorman up to 0.6. This issue affects the function is_safe_url of the file doorman/users/views.py. Executing a manipulation of the argument Next can lead to open redirect. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.	4.3	More Details
CVE-2026-2216	A flaw has been found in rachelos WeRSS we-mp-rss up to 1.4.8. Impacted is the function download_export_file of the file apis/tools.py. Executing a manipulation of the argument filename can lead to path traversal. The attack can be launched remotely. The exploit has been published and may be used.	4.3	More Details
CVE-2025-15333	Tanium addressed an information disclosure vulnerability in Threat Response.	4.3	More Details
CVE-2025-15335	Tanium addressed an information disclosure vulnerability in Threat Response.	4.3	More Details
CVE-2026-1927	The Greenshift – animation and page builder blocks plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the greenshift_app_pass_validation() function in all versions up to, and including, 12.5.7. This makes it possible for authenticated attackers, with Subscriber-level access and above, to retrieve global plugin settings including stored AI API keys.	4.3	More Details
CVE-2025-15342	Tanium addressed an improper access controls vulnerability in Reputation.	4.3	More Details
CVE-2026-25916	Roundcube Webmail before 1.5.13 and 1.6 before 1.6.13, when "Block remote images" is used, does not block SVG feImage.	4.3	More Details
CVE-2020-37145	HRSALE 1.1.8 contains a cross-site request forgery vulnerability that allows attackers to add unauthorized administrative users through the employee registration form. Attackers can craft a malicious HTML page with hidden form fields to trick authenticated administrators into creating new user accounts with elevated privileges.	4.3	More Details
CVE-2026-2160	A vulnerability has been found in SourceCodester Simple Responsive Tourism Website 1.0. Affected by this vulnerability is an unknown functionality of the file /tourism/classes/Master.php?f=save_package. The manipulation of the argument Title leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2026-1964	A vulnerability was determined in WeKan up to 8.20. This impacts an unknown function of the file models/boards.js of the component REST Endpoint. This manipulation causes improper access controls. Remote exploitation of the attack is possible. Upgrading to version 8.21 will fix this issue. Patch name: 545566f5663545d16174e0f2399f231aa693ab6e. It is advisable to upgrade the affected component.	4.3	More Details

CVE-2020-37079	Wing FTP Server versions prior to 6.2.7 contain a cross-site request forgery (CSRF) vulnerability in the web administration interface that allows attackers to delete admin users. Attackers can craft a malicious HTML page with a hidden form to submit a request that deletes the administrative user account without proper authorization.	4.3	More Details
CVE-2025-62439	An Improper Verification of Source of a Communication Channel vulnerability [CWE-940] vulnerability in Fortinet FortiOS 7.6.0 through 7.6.4, FortiOS 7.4.0 through 7.4.9, FortiOS 7.2 all versions, FortiOS 7.0 all versions may allow an authenticated user with knowledge of FSSO policy configurations to gain unauthorized access to protected network resources via crafted requests.	4.2	More Details
CVE-2026-0598	A security flaw was identified in the Ansible Lightspeed API conversation endpoints that handle AI chat interactions. The APIs do not properly verify whether a conversation identifier belongs to the authenticated user making the request. As a result, an attacker with valid credentials could access or influence conversations owned by other users. This exposes sensitive conversation data and allows unauthorized manipulation of AI-generated outputs.	4.2	More Details
CVE-2026-2010	A vulnerability has been found in Sanluan PublicCMS up to 4.0.202506.d/5.202506.d/6.202506.d. Impacted is the function Paid of the file publiccms-parent/publiccms-trade/src/main/java/com/publiccms/logic/service/trade/TradePaymentService.java of the component Trade Payment Handler. The manipulation of the argument paymentId leads to improper authorization. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitability is considered difficult. The exploit has been disclosed to the public and may be used. The identifier of the patch is 7329437e1288540336b1c66c114ed3363adcba02. It is recommended to apply a patch to fix this issue.	4.2	More Details
CVE-2026-1554	XML Injection (aka Blind XPath Injection) vulnerability in Drupal Central Authentication System (CAS) Server allows Privilege Escalation.This issue affects Central Authentication System (CAS) Server: from 0.0.0 before 2.0.3, from 2.1.0 before 2.1.2.	4.2	More Details
CVE-2026-22247	GLPI is a free asset and IT management software package. From version 11.0.0 to before 11.0.5, a GLPI administrator can perform SSRF request through the Webhook feature. This issue has been patched in version 11.0.5.	4.1	More Details
CVE-2025-32467	Use of uninitialized variable for some TDX Module before version tdx1.5 within Ring 0: Hypervisor may allow an information disclosure. Authorized adversary with a privileged user combined with a high complexity attack may enable data exposure. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (high), integrity (none) and availability (none) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	4.1	More Details
CVE-2025-27940	Out-of-bounds read for some TDX Module before version tdx1.5 within Ring 0: Hypervisor may allow an information disclosure. Software side channel adversary with a privileged user combined with a high complexity attack may enable data exposure. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (high), integrity (none) and availability (none) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	4.1	More Details
CVE-2025-27708	Out-of-bounds read in the firmware for some Intel(R) Converged Security and Management Engine (CSME) Firmware (FW) within Ring 0: Kernel may allow an information disclosure. System software adversary with a privileged user combined with a low complexity attack may enable data exposure. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (high), integrity (none) and availability (none) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	4.1	More Details

CVE-2025-27572	Exposure of sensitive information during transient execution for some TDX within Ring 0: Hypervisor may allow an information disclosure. Authorized adversary with a privileged user combined with a high complexity attack may enable data exposure. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (high), integrity (none) and availability (none) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	4.1	More Details
CVE-2026-24914	Type confusion vulnerability in the camera module. Impact: Successful exploitation of this vulnerability may affect availability.	4.0	More Details
CVE-2026-20056	A vulnerability in the Dynamic Vectoring and Streaming (DVS) Engine implementation of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass the anti-malware scanner, allowing malicious archive files to be downloaded. This vulnerability is due to improper handling of certain archive files. An attacker could exploit this vulnerability by sending a crafted archive file, which should be blocked, through an affected device. A successful exploit could allow the attacker to bypass the anti-malware scanner and download malware onto an end user workstation. The downloaded malware will not automatically execute unless the end user extracts and launches the malicious file.	4.0	More Details
CVE-2025-31648	Improper handling of values in the microcode flow for some Intel(R) Processor Family may allow an escalation of privilege. Startup code and smm adversary with a privileged user combined with a high complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are present with special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (low), integrity (low) and availability (none) of the vulnerable system, resulting in subsequent system confidentiality (low), integrity (low) and availability (none) impacts.	3.9	More Details
CVE-2025-22873	It was possible to improperly access the parent directory of an os.Root by opening a filename ending in "../". For example, Root.Open("../") would open the parent directory of the Root. This escape only permits opening the parent directory itself, not ancestors of the parent or files contained within the parent.	3.8	More Details
CVE-2026-2215	A vulnerability was detected in rachelos WeRSS we-mp-rss up to 1.4.8. This issue affects some unknown processing of the file core/auth.py of the component JWT Handler. Performing a manipulation of the argument SECRET_KEY results in use of default cryptographic key. The attack can be initiated remotely. The attack is considered to have high complexity. The exploitability is assessed as difficult. The exploit is now public and may be used.	3.7	More Details
CVE-2025-68157	Webpack is a module bundler. From version 5.49.0 to before 5.104.0, when experiments.buildHttp is enabled, webpack's HTTP(S) resolver (HttpUriPlugin) enforces allowedUris only for the initial URL, but does not re-validate allowedUris after following HTTP 30x redirects. As a result, an import that appears restricted to a trusted allow-list can be redirected to HTTP(S) URLs outside the allow-list. This is a policy/allow-list bypass that enables build-time SSRF behavior (requests from the build machine to internal-only endpoints, depending on network access) and untrusted content inclusion in build outputs (redirected content is treated as module source and bundled). This issue has been patched in version 5.104.0.	3.7	More Details
CVE-2025-15323	Tanium addressed an improper certificate validation vulnerability in Tanium Appliance.	3.7	More Details
CVE-2026-	A security flaw has been discovered in Tasin1025 SwiftBuy up to 0f5011372e8d1d7edfd642d57d721c9fadc54ec7. Affected by this vulnerability is an unknown functionality of the file /login.php. Performing a manipulation results in improper restriction of excessive authentication attempts. Remote exploitation of the attack is possible. The attack's complexity is rated as high. The exploitation appears to be difficult.	3.7	More Details

2110	The exploit has been released to the public and may be used for attacks. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2026-26013	LangChain is a framework for building agents and LLM-powered applications. Prior to 1.2.11, the ChatOpenAI.get_num_tokens_from_messages() method fetches arbitrary image_url values without validation when computing token counts for vision-enabled models. This allows attackers to trigger Server-Side Request Forgery (SSRF) attacks by providing malicious image URLs in user input. This vulnerability is fixed in 1.2.11.	3.7	More Details
CVE-2025-68458	Webpack is a module bundler. From version 5.49.0 to before 5.104.1, when experiments.buildHttp is enabled, webpack's HTTP(S) resolver (HttpUriPlugin) can be bypassed to fetch resources from hosts outside allowedUris by using crafted URLs that include userinfo (username:password@host). If allowedUris enforcement relies on a raw string prefix check (e.g., uri.startsWith(allowed)), a URL that looks allow-listed can pass validation while the actual network request is sent to a different authority/host after URL parsing. This is a policy/allow-list bypass that enables build-time SSRF behavior (outbound requests from the build machine to internal-only endpoints, depending on network access) and untrusted content inclusion (the fetched response is treated as module source and bundled). This issue has been patched in version 5.104.1.	3.7	More Details
CVE-2026-23738	Asterisk is an open source private branch exchange and telephony toolkit. Prior to versions 20.7-cert9, 20.18.2, 21.12.1, 22.8.2, and 23.2.2, user supplied/control values for Cookies and any GET variable query Parameter are directly interpolated into the HTML of the page using ast_str_append. The endpoint at GET /httpstatus is the potential vulnerable endpoint relating to asterisk/main /http.c. This issue has been patched in versions 20.7-cert9, 20.18.2, 21.12.1, 22.8.2, and 23.2.2.	3.5	More Details
CVE-2025-1823	IBM Jazz Reporting Service could allow an authenticated user on the host network to cause a denial of service using specially crafted SQL query that consumes excess memory resources.	3.5	More Details
CVE-2026-2224	A vulnerability was detected in code-projects Online Reviewer System 1.0. This affects an unknown part of the file /system/system/admins/manage/users/btn_functions.php. The manipulation of the argument firstname results in cross site scripting. It is possible to launch the attack remotely. The exploit is now public and may be used.	3.5	More Details
CVE-2026-1970	A flaw has been found in Edimax BR-6258n up to 1.18. This issue affects the function formStaDrvSetup of the file /goform/formStaDrvSetup. This manipulation of the argument submit-url causes open redirect. The attack can be initiated remotely. The exploit has been published and may be used. The vendor confirms that the affected product is end-of-life. They confirm that they "will issue a consolidated Security Advisory on our official support website." This vulnerability only affects products that are no longer supported by the maintainer.	3.5	More Details
CVE-2025-27550	IBM Jazz Reporting Service could allow an authenticated user on the host network to obtain sensitive information about other projects that reside on the server.	3.5	More Details
CVE-2025-2134	IBM Jazz Reporting Service could allow an authenticated user on the network to affect the system's performance using complicated queries due to insufficient resource pooling.	3.5	More Details
CVE-2026-25764	OpenProject is an open-source, web-based project management software. Prior to versions 16.6.7 and 17.0.3, an HTML injection vulnerability occurs in the time tracking function of OpenProject. The application does not escape HTML tags, an attacker with administrator privileges can create a work package with the name containing the HTML tags and add it to the Work package section when creating time tracking. This issue has been patched in versions 16.6.7 and 17.0.3.	3.5	More Details
CVE-	A vulnerability was identified in Portabilis i-Educar up to 2.10. Affected by this vulnerability is an unknown functionality of the file /intranet/meusdadod.php of the component User Data		

2026-2064	Page. Such manipulation of the argument File leads to cross site scripting. 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.	3.5	More Details
CVE-2020-37118	P5 FNIP-8x16A FNIP-4xSH 1.0.20 contains a cross-site request forgery vulnerability that allows attackers to perform administrative actions without user interaction. Attackers can craft malicious web pages to add new admin users, change passwords, and modify system configurations by tricking authenticated users into loading a specially crafted page.	3.5	More Details
CVE-2020-37148	P5 FNIP-8x16A/FNIP-4xSH versions 1.0.20 and 1.0.11 suffer from a stored cross-site scripting vulnerability. Input passed to several GET/POST parameters is not properly sanitized before being returned to the user, allowing attackers to execute arbitrary HTML and script code in a user's browser session in the context of the affected site. This can be exploited by submitting crafted input to the label modification functionality, such as the 'lab4' parameter in config.html.	3.5	More Details
CVE-2026-2145	A vulnerability was identified in cym1102 nginxWebUI up to 4.3.7. The impacted element is an unknown function of the file /adminPage/conf/check of the component Web Management Interface. Such manipulation of the argument nginxDir leads to cross site scripting. 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.	3.5	More Details
CVE-2026-23686	Due to a CRLF Injection vulnerability in SAP NetWeaver Application Server Java, an authenticated attacker with administrative access could submit specially crafted content to the application. If processed by the application, this content enables injection of untrusted entries into generated configuration, allowing manipulation of application-controlled settings. Successful exploitation leads to a low impact on integrity, while confidentiality and availability remain unaffected.	3.4	More Details
CVE-2026-2242	A vulnerability was determined in janet-lang janet up to 1.40.1. This impacts the function janetc_if of the file src/core/specials.c. Executing a manipulation can lead to out-of-bounds read. The attack needs to be launched locally. The exploit has been publicly disclosed and may be utilized. This patch is called c43e06672cd9dacf2122c99f362120a17c34b391. It is advisable to implement a patch to correct this issue.	3.3	More Details
CVE-2026-2241	A vulnerability was found in janet-lang janet up to 1.40.1. This affects the function os_strftime of the file src/core/os.c. Performing a manipulation results in out-of-bounds read. The attack must be initiated from a local position. The exploit has been made public and could be used. The patch is named 0f285855f0e34f9183956be5f16e045f54626bff. To fix this issue, it is recommended to deploy a patch.	3.3	More Details
CVE-2026-2246	A security vulnerability has been detected in AprilRobotics apriltag up to 3.4.5. Affected by this vulnerability is the function apriltag_detector_detect of the file apriltag.c. The manipulation leads to memory corruption. The attack must be carried out locally. The exploit has been disclosed publicly and may be used. The identifier of the patch is cfac2f5ce1ffe2de25967eb1ab80bc5d99fc1a61. It is suggested to install a patch to address this issue.	3.3	More Details
CVE-2026-21249	External control of file name or path in Windows NTLM allows an unauthorized attacker to perform spoofing locally.	3.3	More Details
CVE-2025-15320	Tanium addressed a denial of service vulnerability in Tanium Client.	3.3	More Details
CVE-2026-2245	A vulnerability was identified in CCExtractor up to 183. This affects the function parse_PAT/parse_PMT in the library src/lib_ccx/ts_tables.c of the component MPEG-TS File Parser. Such manipulation leads to out-of-bounds read. The attack can only be performed from a local environment. The exploit is publicly available and might be used. The name of the patch is fd7271bae238ccb3ae8a71304ea64f0886324925. It is best practice to apply a patch to resolve this issue.	3.3	More Details

CVE-2026-1991	A vulnerability was detected in libuvc up to 0.0.7. Affected is the function uvc_scan_streaming of the file src/device.c of the component UVC Descriptor Handler. The manipulation results in null pointer dereference. The attack needs to be approached locally. The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	3.3	More Details
CVE-2026-2259	A vulnerability has been found in aardappel lobster up to 2025.4. Affected by this issue is the function lobster::Parser::ParseStatements in the library dev/src/lobster/parser.h of the component Parsing. The manipulation leads to memory corruption. The attack can only be performed from a local environment. The exploit has been disclosed to the public and may be used. The identifier of the patch is 2f45fe860d00990e79e13250251c1dde633f1f89. Applying a patch is the recommended action to fix this issue.	3.3	More Details
CVE-2025-15571	A security vulnerability has been detected in ckolivas lrzip up to 0.651. This vulnerability affects the function ucompthread of the file stream.c. Such manipulation leads to null pointer dereference. The attack can only be performed from a local environment. 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.	3.3	More Details
CVE-2026-1990	A security vulnerability has been detected in oatpp up to 1.3.1. This impacts the function oatpp::data::type::ObjectWrapper::ObjectWrapper of the file src/oatpp/data/type/Type.hpp. The manipulation leads to null pointer dereference. Local access is required to approach this attack. 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.	3.3	More Details
CVE-2025-25058	Improper initialization for some ESXi kernel mode driver for the Intel(R) Ethernet 800-Series before version 2.2.2.0 (esxi 8.0) & 2.2.3.0 (esxi 9.0) within Ring 1: Device Drivers may allow an information disclosure. Unprivileged software adversary with an authenticated user combined with a low complexity attack may enable data exposure. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (low), integrity (none) and availability (none) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	3.3	More Details
CVE-2026-2258	A flaw has been found in aardappel lobster up to 2025.4. Affected by this vulnerability is the function WaveFunctionCollapse in the library dev/src/lobster/wfc.h. Executing a manipulation can lead to memory corruption. The attack can only be executed locally. The exploit has been published and may be used. This patch is called c2047a33e1ac2c42ab7e8704b33f7ea518a11ffd. It is advisable to implement a patch to correct this issue.	3.3	More Details
CVE-2026-2240	A vulnerability has been found in janet-lang janet up to 1.40.1. The impacted element is the function janetc_pop_funcdef of the file src/core/compile.c. Such manipulation leads to out-of-bounds read. The attack must be carried out locally. The exploit has been disclosed to the public and may be used. The name of the patch is 4dd08a4cdef5b1c42d9a2c19fc24412e97ef51d5. A patch should be applied to remediate this issue.	3.3	More Details
CVE-2026-2069	A flaw has been found in ggml-org llama.cpp up to 55abc39. Impacted is the function llama_grammar_advance_stack of the file llama.cpp/src/llama-grammar.cpp of the component GBNF Grammar Handler. This manipulation causes stack-based buffer overflow. The attack needs to be launched locally. The exploit has been published and may be used. Patch name: 18993. To fix this issue, it is recommended to deploy a patch.	3.3	More Details
CVE-2026-20730	A vulnerability exists in BIG-IP Edge Client and browser VPN clients on Windows that may allow attackers to gain access to sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	3.3	More Details
CVE-2025-	A vulnerability has been found in Mapnik up to 4.2.0. This vulnerability affects the function mapnik::detail::mod<...>::operator of the file src/value.cpp. The manipulation leads to divide by zero. The attack needs to be performed locally. The exploit has been disclosed to	3.3	More Details

15564	the public and may be used. The project was informed of the problem early through an issue report but has not responded yet.		
CVE-2025-15572	A vulnerability has been found in wasm3 up to 0.5.0. The affected element is the function NewCodePage. The manipulation leads to memory leak. The attack must be carried out locally. The exploit has been disclosed to the public and may be used. Unfortunately, the project has no active maintainer at the moment.	3.3	More Details
CVE-2026-1998	A flaw has been found in micropython up to 1.27.0. This vulnerability affects the function mp_import_all of the file py/runtime.c. This manipulation causes memory corruption. The attack needs to be launched locally. The exploit has been published and may be used. Patch name: 570744d06c5ba9dba59b4c3f432ca4f0abd396b6. It is suggested to install a patch to address this issue.	3.3	More Details
CVE-2025-33030	Improper conditions check in some firmware for some Intel(R) NPU Drivers within Ring 3: User Applications may allow an escalation of privilege. Unprivileged software adversary with an authenticated user combined with a low complexity attack may enable data corruption. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (none), integrity (low) and availability (none) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	3.3	More Details
CVE-2026-25815	Fortinet FortiOS through 7.6.6 allows attackers to decrypt LDAP credentials stored in device configuration files, as exploited in the wild from 2025-12-16 through 2026 (by default, the encryption key is the same across all customers' installations). NOTE: the Supplier's position is that the instance of CWE-1394 is not a vulnerability because customers "are supposed to enable" a non-default option that eliminates the weakness. However, that non-default option can disrupt functionality as shown in the "Managing FortiGates with private data encryption" document, and is therefore intentionally not a default option.	3.2	More Details
CVE-2026-20732	A vulnerability exists in an undisclosed BIG-IP Configuration utility page that may allow an attacker to spoof error messages. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	3.1	More Details
CVE-2026-24320	Due to improper memory management in SAP NetWeaver and ABAP Platform (Application Server ABAP), an authenticated attacker could exploit logical errors in memory management by supplying specially crafted input containing unique characters, which are improperly converted. This may result in memory corruption and the potential leakage of memory content. Successful exploitation of this vulnerability would have a low impact on the confidentiality of the application, with no effect on its integrity or availability.	3.1	More Details
CVE-2025-15289	Tanium addressed an improper access controls vulnerability in Interact.	3.1	More Details
CVE-2026-1762	A vulnerability in GE Vernova Enervista UR Setup on Windows allows File Manipulation.This issue affects Enervista: 8.6 and prior versions.	2.9	More Details
CVE-2025-32739	Improper conditions check in some firmware for some Intel(R) Graphics Drivers and Intel LTS kernels within Ring 1: Device Drivers may allow a denial of service. Unprivileged software adversary with an authenticated user combined with a high complexity attack may enable denial of service. This result may potentially occur via local access when attack requirements are present with special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (none), integrity (none) and availability (low) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	2.8	More Details
CVE-2026-1791	Unrestricted Upload of File with Dangerous Type vulnerability in Hillstone Networks Operation and Maintenance Security Gateway on Linux allows Upload a Web Shell to a Web Server.This issue affects Operation and Maintenance Security Gateway: V5.5ST00001B113.	2.7	More Details

CVE-2025-15321	Tanium addressed an improper input validation vulnerability in Tanium Appliance.	2.7	More Details
CVE-2026-2200	A weakness has been identified in heyewei JFinalCMS 5.0.0. This affects an unknown function of the file /admin/admin/save of the component API Endpoint. Executing a manipulation 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.	2.4	More Details
CVE-2026-2156	A weakness has been identified in code-projects Online Student Management System 1.0. The impacted element is an unknown function of the file /admin/announcement/index.php?view=add of the component Announcement Management Module. This manipulation causes cross site scripting. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks.	2.4	More Details
CVE-2026-2201	A security vulnerability has been detected in ZeroWdd studentmanager up to 2151560fc0a50ec00426785ec1e01a3763b380d9. This impacts the function addLeave of the file src/main/java/com/wdd/studentmanager/controller/LeaveController.java. The manipulation of the argument Reason for Leave leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used. This product uses a rolling release model to deliver continuous updates. As a result, specific version information for affected or updated releases is not available. The code repository of the project has not been active for many years.	2.4	More Details
CVE-2026-1971	A vulnerability has been found in Edimax BR-6288ACL up to 1.12. Impacted is the function wiz_WISP24gmanual of the file wiz_WISP24gmanual.asp. Such manipulation of the argument manualssid leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor confirms that the affected product is end-of-life. They confirm that they "will issue a consolidated Security Advisory on our official support website." This vulnerability only affects products that are no longer supported by the maintainer.	2.4	More Details
CVE-2026-2214	A weakness has been identified in code-projects for Plugin 1.0. This affects an unknown part of the file /Administrator/PHP/AdminAddAlbum.php. This manipulation of the argument txtalbum causes cross site scripting. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks.	2.4	More Details
CVE-2026-2222	A weakness has been identified in code-projects Online Reviewer System 1.0. Affected by this vulnerability is an unknown functionality of the file /system/system/admins/manage/users/btn_functions.php. Executing a manipulation of the argument firstname can lead to cross site scripting. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks.	2.4	More Details
CVE-2026-23739	Asterisk is an open source private branch exchange and telephony toolkit. Prior to versions 20.7-cert9, 20.18.2, 21.12.1, 22.8.2, and 23.2.2, the ast_xml_open() function in xml.c parses XML documents using libxml with unsafe parsing options that enable entity expansion and XInclude processing. Specifically, it invokes xmlReadFile() with the XML_PARSE_NOENT flag and later processes XIncludes via xmlXIncludeProcess().If any untrusted or user-supplied XML file is passed to this function, it can allow an attacker to trigger XML External Entity (XXE) or XInclude-based local file disclosure, potentially exposing sensitive files from the host system. This can also be triggered in other cases in which the user is able to supply input in xml format that triggers the asterisk process to parse it. This issue has been patched in versions 20.7-cert9, 20.18.2, 21.12.1, 22.8.2, and 23.2.2.	2.0	More Details
CVE-2026-23740	Asterisk is an open source private branch exchange and telephony toolkit. Prior to versions 20.7-cert9, 20.18.2, 21.12.1, 22.8.2, and 23.2.2, when ast_coredumper writes its gdb init and output files to a directory that is world-writable (for example /tmp), an attacker with write permission(which is all users on a linux system) to that directory can cause root to execute arbitrary commands or overwrite arbitrary files by controlling the gdb init file and output paths. This issue has been patched in versions 20.7-cert9, 20.18.2, 21.12.1, 22.8.2, and 23.2.2.	0.0	More Details
	Winter is a free, open-source content management system (CMS) based on the Laravel PHP		

CVE-2026-22254	framework. Versions of Winter CMS before 1.2.10 allow users with access to the CMS Asset Manager were able to upload SVGs without automatic sanitization. To actively exploit this security issue, an attacker would need access to the Backend with a user account with the following permission: cms.manage_assets. The Winter CMS maintainers strongly recommend that the cms.manage_assets permission only be reserved to trusted administrators and developers in general. This vulnerability is fixed in 1.2.10.	0.0	More Details
CVE-2026-23741	Asterisk is an open source private branch exchange and telephony toolkit. Prior to versions 20.7-cert9, 20.18.2, 21.12.1, 22.8.2, and 23.2.2, the asterisk/contrib/scripts/ast_coredumper runs as root, as noted by the NOTES tag on line 689 of the ast_coredumper file. The script will source the contents of /etc/asterisk/ast_debug_tools.conf, which resides in a folder that is writeable by the asterisk user:group. Due to the /etc/asterisk/ast_debug_tools.conf file following bash semantics and it being loaded; an attacker with write permissions may add or modify the file such that when the root ast_coredumper is run; it would source and thereby execute arbitrary bash code found in the /etc/asterisk/ast_debug_tools.conf. This issue has been patched in versions 20.7-cert9, 20.18.2, 21.12.1, 22.8.2, and 23.2.2.	0.0	More Details
CVE-2026-23073	In the Linux kernel, the following vulnerability has been resolved: wifi: rsi: Fix memory corruption due to not set vif driver data size The struct ieee80211_vif contains trailing space for vif driver data, when struct ieee80211_vif is allocated, the total memory size that is allocated is sizeof(struct ieee80211_vif) + size of vif driver data. The size of vif driver data is set by each WiFi driver as needed. The RSI911x driver does not set vif driver data size, no trailing space for vif driver data is therefore allocated past struct ieee80211_vif . The RSI911x driver does however use the vif driver data to store its vif driver data structure "struct vif_priv". An access to vif->drv_priv leads to access out of struct ieee80211_vif bounds and corruption of some memory. In case of the failure observed locally, rsi_mac80211_add_interface() would write struct vif_priv *vif_info = (struct vif_priv *)vif->drv_priv; vif_info->vap_id = vap_idx. This write corrupts struct fq_tin member struct list_head new_flows . The flow = list_first_entry(head, struct fq_flow, flowchain); in fq_tin_reset() then reports non-NULL bogus address, which when accessed causes a crash. The trigger is very simple, boot the machine with init=/bin/sh , mount devtmpfs, sysfs, procfs, and then do "ip link set wlan0 up", "sleep 1", "ip link set wlan0 down" and the crash occurs. Fix this by setting the correct size of vif driver data, which is the size of "struct vif_priv", so that memory is allocated and the driver can store its driver data in it, instead of corrupting memory around it.	N/A	More Details
CVE-2026-23072	In the Linux kernel, the following vulnerability has been resolved: l2tp: Fix memleak in l2tp_udp_encap_recv(). syzbot reported memleak of struct l2tp_session, l2tp_tunnel, sock, etc. [0] The cited commit moved down the validation of the protocol version in l2tp_udp_encap_recv(). The new place requires an extra error handling to avoid the memleak. Let's call l2tp_session_put() there. [0]: BUG: memory leak unreferenced object 0xffff88810a290200 (size 512): comm "syz.0.17", pid 6086, jiffies 4294944299 hex dump (first 32 bytes): 7d eb 04 0c 00 00 00 00 01 00 00 00 00 00 00 00 }..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... backtrace (crc babb6a4f): kmemleak_alloc_recursive include/linux/kmemleak.h:44 [inline] slab_post_alloc_hook mm/slub.c:4958 [inline] slab_alloc_node mm/slub.c:5263 [inline] __do_kmalloc_node mm/slub.c:5656 [inline] __kmalloc_noprof+0x3e0/0x660 mm/slub.c:5669 kmalloc_noprof include/linux/slab.h:961 [inline] kzalloc_noprof include/linux/slab.h:1094 [inline] l2tp_session_create+0x3a/0x3b0 net/l2tp/l2tp_core.c:1778 pppol2tp_connect+0x48b/0x920 net/l2tp/l2tp_ppp.c:755 __sys_connect_file+0x7a/0xb0 net/socket.c:2089 __sys_connect+0xde/0x110 net/socket.c:2108 __do_sys_connect net/socket.c:2114 [inline] __se_sys_connect net/socket.c:2111 [inline] __x64_sys_connect+0x1c/0x30 net/socket.c:2111 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xa4/0xf80 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f	N/A	More Details
CVE-2026-23083	In the Linux kernel, the following vulnerability has been resolved: fou: Don't allow 0 for FOU_ATTR_IPPROTO. fou_udp_recv() has the same problem mentioned in the previous patch. If FOU_ATTR_IPPROTO is set to 0, skb is not freed by fou_udp_recv() nor "resubmit"-ted in ip_protocol_deliver_rcu(). Let's forbid 0 for FOU_ATTR_IPPROTO.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: drm/panel-simple: fix		

CVE-2026-23049	connector type for DataImage SCF0700C48GGU18 panel The connector type for the DataImage SCF0700C48GGU18 panel is missing and devm_drm_panel_bridge_add() requires connector type to be set. This leads to a warning and a backtrace in the kernel log and panel does not work: " WARNING: CPU: 3 PID: 38 at drivers/gpu/drm/bridge/panel.c:379 devm_drm_of_get_bridge+0xac/0xb8 " The warning is triggered by a check for valid connector type in devm_drm_panel_bridge_add(). If there is no valid connector type set for a panel, the warning is printed and panel is not added. Fill in the missing connector type to fix the warning and make the panel operational once again.	N/A	More Details
CVE-2026-23068	In the Linux kernel, the following vulnerability has been resolved: spi: spi-sprd-adi: Fix double free in probe error path The driver currently uses spi_alloc_host() to allocate the controller but registers it using devm_spi_register_controller(). If devm_register_restart_handler() fails, the code jumps to the put_ctlr label and calls spi_controller_put(). However, since the controller was registered via a devm function, the device core will automatically call spi_controller_put() again when the probe fails. This results in a double-free of the spi_controller structure. Fix this by switching to devm_spi_alloc_host() and removing the manual spi_controller_put() call.	N/A	More Details
CVE-2026-25753	PlaciPy is a placement management system designed for educational institutions. In version 1.0.0, the application uses a hard-coded, static default password for all newly created student accounts. This results in mass account takeover, allowing any attacker to log in as any student once the password is known.	N/A	More Details
CVE-2026-23071	In the Linux kernel, the following vulnerability has been resolved: regmap: Fix race condition in hwspinlock irqsave routine Previously, the address of the shared member '&map->spinlock_flags' was passed directly to 'hwspin_lock_timeout_irqsave'. This creates a race condition where multiple contexts contending for the lock could overwrite the shared flags variable, potentially corrupting the state for the current lock owner. Fix this by using a local stack variable 'flags' to store the IRQ state temporarily.	N/A	More Details
CVE-2026-23065	In the Linux kernel, the following vulnerability has been resolved: platform/x86/amd: Fix memory leak in wbrf_record() The tmp buffer is allocated using kcalloc() but is not freed if acpi_evaluate_dsm() fails. This causes a memory leak in the error path. Fix this by explicitly freeing the tmp buffer in the error handling path of acpi_evaluate_dsm().	N/A	More Details
CVE-2026-23055	In the Linux kernel, the following vulnerability has been resolved: i2c: riic: Move suspend handling to NOIRQ phase Commit 53326135d0e0 ("i2c: riic: Add suspend/resume support") added suspend support for the Renesas I2C driver and following this change on RZ/G3E the following WARNING is seen on entering suspend ... [134.275704] Freezing remaining freezable tasks completed (elapsed 0.001 seconds) [134.285536] ------------[cut here]------------ [134.290298] i2c i2c-2: Transfer while suspended [134.295174] WARNING: drivers/i2c/i2c-core.h:56 at __i2c_smbus_xfer+0x1e4/0x214, CPU#0: systemd-sleep/388 [134.365507] Tainted: [W]=WARN [134.368485] Hardware name: Renesas SMARC EVK version 2 based on r9a09g047e57 (DT) [134.375961] pstate: 60400005 (nZCv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) [134.382935] pc : __i2c_smbus_xfer+0x1e4/0x214 [134.387329] lr : __i2c_smbus_xfer+0x1e4/0x214 [134.391717] sp : ffff800083f23860 [134.395040] x29: ffff800083f23860 x28: 0000000000000000 x27: ffff800082ed5d60 [134.402226] x26: 0000001f4395fd74 x25: 0000000000000007 x24: 0000000000000001 [134.409408] x23: 0000000000000000 x22: 000000000000006f x21: ffff800083f23936 [134.416589] x20: ffff0000c090e140 x19: ffff0000c090e0d0 x18: 0000000000000006 [134.423771] x17: 6f63657320313030 x16: 2e30206465737061 x15: ffff800083f23280 [134.430953] x14: 0000000000000000 x13: ffff800082b16ce8 x12: 0000000000000f09 [134.438134] x11: 0000000000000503 x10: ffff800082b6ece8 x9 : ffff800082b16ce8 [134.445315] x8 : 00000000ffffefff x7 : ffff800082b6ece8 x6 : 80000000fffff000 [134.452495] x5 : 0000000000000504 x4 : 0000000000000000 x3 : 0000000000000000 [134.459672] x2 : 0000000000000000 x1 : 0000000000000000 x0 : ffff0000c9ee9e80 [134.466851] Call trace: [134.469311] __i2c_smbus_xfer+0x1e4/0x214 (P) [134.473715] i2c_smbus_xfer+0xbc/0x120 [134.477507] i2c_smbus_read_byte_data+0x4c/0x84 [134.482077] isl1208_i2c_read_time+0x44/0x178 [rtc_isl1208] [134.487703] isl1208_rtc_read_time+0x14/0x20 [rtc_isl1208] [134.493226] __rtc_read_time+0x44/0x88 [134.497012] rtc_read_time+0x3c/0x68 [134.500622] rtc_suspend+0x9c/0x170 The warning is triggered because I2C transfers can still be attempted while the controller is already suspended, due to inappropriate ordering of the system sleep callbacks. If the	N/A	More Details

	already suspended, add to inappropriate ordering of the system sleep callbacks. If the controller is autosuspended, there is no way to wake it up once runtime PM disabled (in suspend_late()). During system resume, the I2C controller will be available only after runtime PM is re-enabled (in resume_early()). However, this may be too late for some devices. Wake up the controller in the suspend() callback while runtime PM is still enabled. The I2C controller will remain available until the suspend_noirq() callback (pm_runtime_force_suspend()) is called. During resume, the I2C controller can be restored by the resume_noirq() callback (pm_runtime_force_resume()). Finally, the resume() callback re-enables autosuspend. As a result, the I2C controller can remain available until the system enters suspend_noirq() and from resume_noirq().		
CVE-2026-23067	In the Linux kernel, the following vulnerability has been resolved: iommu/io-pgtable-arm: fix size_t signedness bug in unmap path __arm_lpae_unmap() returns size_t but was returning -ENOENT (negative error code) when encountering an unmapped PTE. Since size_t is unsigned, -ENOENT (typically -2) becomes a huge positive value (0xFFFFFFFFFFFFFFFE on 64-bit systems). This corrupted value propagates through the call chain: __arm_lpae_unmap() returns -ENOENT as size_t -> arm_lpae_unmap_pages() returns it -> __iommu_unmap() adds it to iova address -> iommu_pgsize() triggers BUG_ON due to corrupted iova This can cause IOVA address overflow in __iommu_unmap() loop and trigger BUG_ON in iommu_pgsize() from invalid address alignment. Fix by returning 0 instead of -ENOENT. The WARN_ON already signals the error condition, and returning 0 (meaning "nothing unmapped") is the correct semantic for size_t return type. This matches the behavior of other io-pgtable implementations (io-pgtable-arm-v7s, io-pgtable-dart) which return 0 on error conditions.	N/A	More Details
CVE-2026-23058	In the Linux kernel, the following vulnerability has been resolved: can: ems_usb: ems_usb_read_bulk_callback(): fix URB memory leak Fix similar memory leak as in commit 7352e1d5932a ("can: gs_usb: gs_usb_receive_bulk_callback(): fix URB memory leak"). In ems_usb_open(), the URBs for USB-in transfers are allocated, added to the dev->rx_submitted anchor and submitted. In the complete callback ems_usb_read_bulk_callback(), the URBs are processed and resubmitted. In ems_usb_close() the URBs are freed by calling usb_kill_anchored_urbs(&dev->rx_submitted). However, this does not take into account that the USB framework unanchors the URB before the complete function is called. This means that once an in-URB has been completed, it is no longer anchored and is ultimately not released in ems_usb_close(). Fix the memory leak by anchoring the URB in the ems_usb_read_bulk_callback() to the dev->rx_submitted anchor.	N/A	More Details
CVE-2026-23069	In the Linux kernel, the following vulnerability has been resolved: vsock/virtio: fix potential underflow in virtio_transport_get_credit() The credit calculation in virtio_transport_get_credit() uses unsigned arithmetic: ret = vvs->peer_buf_alloc - (vvs->tx_cnt - vvs->peer_fwd_cnt); If the peer shrinks its advertised buffer (peer_buf_alloc) while bytes are in flight, the subtraction can underflow and produce a large positive value, potentially allowing more data to be queued than the peer can handle. Reuse virtio_transport_has_space() which already handles this case and add a comment to make it clear why we are doing that. [Stefano: use virtio_transport_has_space() instead of duplicating the code] [Stefano: tweak the commit message]	N/A	More Details
CVE-2026-23056	In the Linux kernel, the following vulnerability has been resolved: uacce: implement mremap in uacce_vm_ops to return -EPERM The current uacce_vm_ops does not support the mremap operation of vm_operations_struct. Implement .mremap to return -EPERM to remind users. The reason we need to explicitly disable mremap is that when the driver does not implement .mremap, it uses the default mremap method. This could lead to a risk scenario: An application might first mmap address p1, then mremap to p2, followed by munmap(p1), and finally munmap(p2). Since the default mremap copies the original vma's vm_private_data (i.e., q) to the new vma, both munmap operations would trigger vma_close, causing q->qfr to be freed twice(qfr will be set to null here, so repeated release is ok).	N/A	More Details
CVE-2026-25650	MCP Salesforce Connector is a Model Context Protocol (MCP) server implementation for Salesforce integration. Prior to 0.1.10, arbitrary attribute access leads to disclosure of Salesforce auth token. This vulnerability is fixed in 0.1.10.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: rxrpc: Fix recvmsg() unconditional requeue If rxrpc_recvmsg() fails because MSG_DONTWAIT was specified but the call at the front of the recvmsg queue already has its mutex locked, it requeues the call		

CVE-2026-23066	- whether or not the call is already queued. The call may be on the queue because MSG_PEEK was also passed and so the call was not dequeued or because the I/O thread requeued it. The unconditional requeue may then corrupt the recvmsg queue, leading to things like UAFs or refcount underruns. Fix this by only requeuing the call if it isn't already on the queue - and moving it to the front if it is already queued. If we don't queue it, we have to put the ref we obtained by dequeuing it. Also, MSG_PEEK doesn't dequeue the call so shouldn't call rxrpc_notify_socket() for the call if we didn't use up all the data on the queue, so fix that also.	N/A	More Details
CVE-2026-23074	In the Linux kernel, the following vulnerability has been resolved: net/sched: Enforce that teql can only be used as root qdisc Design intent of teql is that it is only supposed to be used as root qdisc. We need to check for that constraint. Although not important, I will describe the scenario that unearthed this issue for the curious. GangMin Kim <km.kim1503@gmail.com> managed to concot a scenario as follows: ROOT qdisc 1:0 (QFQ) ├── class 1:1 (weight=15, lmax=16384) netem with delay 6.4s └── class 1:2 (weight=1, lmax=1514) teql GangMin sends a packet which is enqueued to 1:1 (netem). Any invocation of dequeue by QFQ from this class will not return a packet until after 6.4s. In the meantime, a second packet is sent and it lands on 1:2. teql's enqueue will return success and this will activate class 1:2. Main issue is that teql only updates the parent visible qlen (sch->q.qlen) at dequeue. Since QFQ will only call dequeue if peek succeeds (and teql's peek always returns NULL), dequeue will never be called and thus the qlen will remain as 0. With that in mind, when GangMin updates 1:2's lmax value, the qfq_change_class calls qfq_deact_rm_from_agg. Since the child qdisc's qlen was not incremented, qfq fails to deactivate the class, but still frees its pointers from the aggregate. So when the first packet is rescheduled after 6.4 seconds (netem's delay), a dangling pointer is accessed causing GangMin's causing a UAF.	N/A	More Details
CVE-2026-23064	In the Linux kernel, the following vulnerability has been resolved: net/sched: act_ife: avoid possible NULL deref tcf_ife_encode() must make sure ife_encode() does not return NULL. syzbot reported: Oops: general protection fault, probably for non-canonical address 0xdffffc0000000000: 0000 [#1] SMP KASAN NOPTI KASAN: null-ptr-deref in range [0x0000000000000000-0x0000000000000007] RIP: 0010:ife_tlv_meta_encode+0x41/0xa0 net/ife/ife.c:166 CPU: 3 UID: 0 PID: 8990 Comm: syz.0.696 Not tainted syzkaller #0 PREEMPT(full) Call Trace: <TASK> ife_encode_meta_u32+0x153/0x180 net/sched/act_ife.c:101 tcf_ife_encode net/sched/act_ife.c:841 [inline] tcf_ife_act+0x1022/0x1de0 net/sched/act_ife.c:877 tc_act include/net/tc_wrapper.h:130 [inline] tcf_action_exec+0x1c0/0xa20 net/sched/act_api.c:1152 tcf_exts_exec include/net/pkt_cls.h:349 [inline] mall_classify+0x1a0/0x2a0 net/sched/cls_matchall.c:42 tc_classify include/net/tc_wrapper.h:197 [inline] __tcf_classify net/sched/cls_api.c:1764 [inline] tcf_classify+0x7f2/0x1380 net/sched/cls_api.c:1860 multiq_classify net/sched/sch_multiq.c:39 [inline] multiq_enqueue+0xe0/0x510 net/sched/sch_multiq.c:66 dev_qdisc_enqueue+0x45/0x250 net/core/dev.c:4147 __dev_xmit_skb net/core/dev.c:4262 [inline] __dev_queue_xmit+0x2998/0x46c0 net/core/dev.c:4798	N/A	More Details
CVE-2026-23075	In the Linux kernel, the following vulnerability has been resolved: can: esd_usb: esd_usb_read_bulk_callback(): fix URB memory leak Fix similar memory leak as in commit 7352e1d5932a ("can: gs_usb: gs_usb_receive_bulk_callback(): fix URB memory leak"). In esd_usb_open(), the URBs for USB-in transfers are allocated, added to the dev->rx_submitted anchor and submitted. In the complete callback esd_usb_read_bulk_callback(), the URBs are processed and resubmitted. In esd_usb_close() the URBs are freed by calling usb_kill_anchored_urbs(&dev->rx_submitted). However, this does not take into account that the USB framework unanchors the URB before the complete function is called. This means that once an in-URB has been completed, it is no longer anchored and is ultimately not released in esd_usb_close(). Fix the memory leak by anchoring the URB in the esd_usb_read_bulk_callback() to the dev->rx_submitted anchor.	N/A	More Details
CVE-2026-23054	In the Linux kernel, the following vulnerability has been resolved: net: hv_netvsc: reject RSS hash key programming without RX indirection table RSS configuration requires a valid RX indirection table. When the device reports a single receive queue, rndis_filter_device_add() does not allocate an indirection table, accepting RSS hash key updates in this state leads to a hang. Fix this by gating netvsc_set_rxfh() on ndc->rx_table_sz and return -EOPNOTSUPP when the table is absent. This aligns set_rxfh with the device capabilities and prevents incorrect behavior	N/A	More Details

	incorrect behavior.		
CVE-2026-23078	In the Linux kernel, the following vulnerability has been resolved: ALSA: scarlett2: Fix buffer overflow in config retrieval The scarlett2_usb_get_config() function has a logic error in the endianness conversion code that can cause buffer overflows when count > 1. The code checks `if (size == 2)` where `size` is the total buffer size in bytes, then loops `count` times treating each element as u16 (2 bytes). This causes the loop to access `count * 2` bytes when the buffer only has `size` bytes allocated. Fix by checking the element size (config_item->size) instead of the total buffer size. This ensures the endianness conversion matches the actual element type.	N/A	More Details
CVE-2026-23079	In the Linux kernel, the following vulnerability has been resolved: gpio: cdev: Fix resource leaks on errors in lineinfo_changed_notify() On error handling paths, lineinfo_changed_notify() doesn't free the allocated resources which results leaks. Fix it.	N/A	More Details
CVE-2026-23076	In the Linux kernel, the following vulnerability has been resolved: ALSA: ctxfi: Fix potential OOB access in audio mixer handling In the audio mixer handling code of ctxfi driver, the conf field is used as a kind of loop index, and it's referred in the index callbacks (amixer_index() and sum_index()). As spotted recently by fuzzers, the current code causes OOB access at those functions. | UBSAN: array-index-out-of-bounds in /build/reproducible-path/linux-6.17.8/sound/pci/ctxfi/ctamixer.c:347:48 | index 8 is out of range for type 'unsigned char [8]' After the analysis, the cause was found to be the lack of the proper (re-)initialization of conj field. This patch addresses those OOB accesses by adding the proper initializations of the loop indices.	N/A	More Details
CVE-2026-23070	In the Linux kernel, the following vulnerability has been resolved: Octeontx2-af: Add proper checks for fwdata firmware populates MAC address, link modes (supported, advertised) and EEPROM data in shared firmware structure which kernel access via MAC block(CGX/RPM). Accessing fwdata, on boards booted with out MAC block leading to kernel panics. Internal error: Oops: 0000000096000005 [#1] SMP [10.460721] Modules linked in: [10.463779] CPU: 0 UID: 0 PID: 174 Comm: kworker/0:3 Not tainted 6.19.0-rc5-00154-g76ec646abdf7-dirty #3 PREEMPT [10.474045] Hardware name: Marvell OcteonTX CN98XX board (DT) [10.479793] Workqueue: events work_for_cpu_fn [10.484159] pstate: 80400009 (Nzcv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) [10.491124] pc : rvu_sdp_init+0x18/0x114 [10.495051] lr : rvu_probe+0xe58/0x1d18	N/A	More Details
CVE-2026-23080	In the Linux kernel, the following vulnerability has been resolved: can: mcba_usb: mcba_usb_read_bulk_callback(): fix URB memory leak Fix similar memory leak as in commit 7352e1d5932a ("can: gs_usb: gs_usb_receive_bulk_callback(): fix URB memory leak"). In mcba_usb_probe() -> mcba_usb_start(), the URBs for USB-in transfers are allocated, added to the priv->rx_submitted anchor and submitted. In the complete callback mcba_usb_read_bulk_callback(), the URBs are processed and resubmitted. In mcba_usb_close() -> mcba_urb_unlink() the URBs are freed by calling usb_kill_anchored_urbs(&priv->rx_submitted). However, this does not take into account that the USB framework unanchors the URB before the complete function is called. This means that once an in-URB has been completed, it is no longer anchored and is ultimately not released in usb_kill_anchored_urbs(). Fix the memory leak by anchoring the URB in the mcba_usb_read_bulk_callback()to the priv->rx_submitted anchor.	N/A	More Details
CVE-2026-23061	In the Linux kernel, the following vulnerability has been resolved: can: kvaser_usb: kvaser_usb_read_bulk_callback(): fix URB memory leak Fix similar memory leak as in commit 7352e1d5932a ("can: gs_usb: gs_usb_receive_bulk_callback(): fix URB memory leak"). In kvaser_usb_set_{,data_}bittiming() -> kvaser_usb_setup_rx_urbs(), the URBs for USB-in transfers are allocated, added to the dev->rx_submitted anchor and submitted. In the complete callback kvaser_usb_read_bulk_callback(), the URBs are processed and resubmitted. In kvaser_usb_remove_interfaces() the URBs are freed by calling usb_kill_anchored_urbs(&dev->rx_submitted). However, this does not take into account that the USB framework unanchors the URB before the complete function is called. This means that once an in-URB has been completed, it is no longer anchored and is ultimately not released in usb_kill_anchored_urbs(). Fix the memory leak by anchoring the URB in the kvaser_usb_read_bulk_callback() to the dev->rx_submitted anchor.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: platform/x86: hp-bioscfg:		

CVE-2026-23062	Fix kernel panic in GET_INSTANCE_ID macro The GET_INSTANCE_ID macro that caused a kernel panic when accessing sysfs attributes: 1. Off-by-one error: The loop condition used '<=' instead of '<', causing access beyond array bounds. Since array indices are 0-based and go from 0 to instances_count-1, the loop should use '<'. 2. Missing NULL check: The code dereferenced attr_name_kobj->name without checking if attr_name_kobj was NULL, causing a null pointer dereference in min_length_show() and other attribute show functions. The panic occurred when fwupd tried to read BIOS configuration attributes: Oops: general protection fault [#1] SMP KASAN NOPTI KASAN: null-ptr-deref in range [0x0000000000000000-0x0000000000000007] RIP: 0010:min_length_show+0xcf/0x1d0 [hp_bioscfg] Add a NULL check for attr_name_kobj before dereferencing and corrects the loop boundary to match the pattern used elsewhere in the driver.	N/A	More Details
CVE-2026-23081	In the Linux kernel, the following vulnerability has been resolved: net: phy: intel-xway: fix OF node refcount leakage Automated review spotted am OF node reference count leakage when checking if the 'leds' child node exists. Call of_put_node() to correctly maintain the refcount.	N/A	More Details
CVE-2026-23063	In the Linux kernel, the following vulnerability has been resolved: uacce: ensure safe queue release with state management Directly calling `put_queue` carries risks since it cannot guarantee that resources of `uacce_queue` have been fully released beforehand. So adding a `stop_queue` operation for the UACCE_CMD_PUT_Q command and leaving the `put_queue` operation to the final resource release ensures safety. Queue states are defined as follows: - UACCE_Q_ZOMBIE: Initial state - UACCE_Q_INIT: After opening `uacce` - UACCE_Q_STARTED: After `start` is issued via `ioctl` When executing `poweroff -f` in virt while accelerator are still working, `uacce_fops_release` and `uacce_remove` may execute concurrently. This can cause `uacce_put_queue` within `uacce_fops_release` to access a NULL `ops` pointer. Therefore, add state checks to prevent accessing freed pointers.	N/A	More Details
CVE-2026-23082	In the Linux kernel, the following vulnerability has been resolved: can: gs_usb: gs_usb_receive_bulk_callback(): unanchor URL on usb_submit_urb() error In commit 7352e1d5932a ("can: gs_usb: gs_usb_receive_bulk_callback(): fix URB memory leak"), the URB was re-anchored before usb_submit_urb() in gs_usb_receive_bulk_callback() to prevent a leak of this URB during cleanup. However, this patch did not take into account that usb_submit_urb() could fail. The URB remains anchored and usb_kill_anchored_urbs(&parent->rx_submitted) in gs_can_close() loops infinitely since the anchor list never becomes empty. To fix the bug, unanchor the URB when an usb_submit_urb() error occurs, also print an info message.	N/A	More Details
CVE-2026-23052	In the Linux kernel, the following vulnerability has been resolved: ftrace: Do not over-allocate ftrace memory The pg_remaining calculation in ftrace_process_locs() assumes that ENTRIES_PER_PAGE multiplied by 2^order equals the actual capacity of the allocated page group. However, ENTRIES_PER_PAGE is PAGE_SIZE / ENTRY_SIZE (integer division). When PAGE_SIZE is not a multiple of ENTRY_SIZE (e.g. 4096 / 24 = 170 with remainder 16), high-order allocations (like 256 pages) have significantly more capacity than 256 * 170. This leads to pg_remaining being underestimated, which in turn makes skip (derived from skipped - pg_remaining) larger than expected, causing the WARN(skip != remaining) to trigger. Extra allocated pages for ftrace: 2 with 654 skipped WARNING: CPU: 0 PID: 0 at kernel/trace/ftrace.c:7295 ftrace_process_locs+0x5bf/0x5e0 A similar problem in ftrace_allocate_records() can result in allocating too many pages. This can trigger the second warning in ftrace_process_locs(). Extra allocated pages for ftrace WARNING: CPU: 0 PID: 0 at kernel/trace/ftrace.c:7276 ftrace_process_locs+0x548/0x580 Use the actual capacity of a page group to determine the number of pages to allocate. Have ftrace_allocate_pages() return the number of allocated pages to avoid having to calculate it. Use the actual page group capacity when validating the number of unused pages due to skipped entries. Drop the definition of ENTRIES_PER_PAGE since it is no longer used.	N/A	More Details
CVE-2026-23053	In the Linux kernel, the following vulnerability has been resolved: NFS: Fix a deadlock involving nfs_release_folio() Wang Zhaolong reports a deadlock involving NFSv4.1 state recovery waiting on kthreadd, which is attempting to reclaim memory by calling nfs_release_folio(). The latter cannot make progress due to state recovery being needed. It seems that the only safe thing to do here is to kick off a writeback of the folio, without waiting for completion, or else kicking off an asynchronous commit.	N/A	More Details

CVE-2026-23051	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: fix drm panic null pointer when driver not support atomic When driver not support atomic, fb using plane->fb rather than plane->state->fb. (cherry picked from commit 2f2a72de673513247cd6fae14e53f6c40c5841ef)	N/A	More Details
CVE-2026-23050	In the Linux kernel, the following vulnerability has been resolved: pNFS: Fix a deadlock when returning a delegation during open() Ben Coddington reports seeing a hang in the following stack trace: 0 [ffffd0b50e1774e0] __schedule at ffffffff9ca05415 1 [ffffd0b50e177548] schedule at ffffffff9ca05717 2 [ffffd0b50e177558] bit_wait at ffffffff9ca061e1 3 [ffffd0b50e177568] __wait_on_bit at ffffffff9ca05cfb 4 [ffffd0b50e1775c8] out_of_line_wait_on_bit at ffffffff9ca05ea5 5 [ffffd0b50e177618] pnfs_roc at ffffffffc154207b [nfsv4] 6 [ffffd0b50e1776b8] _nfs4_proc_delegreturn at ffffffffc1506586 [nfsv4] 7 [ffffd0b50e177788] nfs4_proc_delegreturn at ffffffffc1507480 [nfsv4] 8 [ffffd0b50e1777f8] nfs_do_return_delegation at ffffffffc1523e41 [nfsv4] 9 [ffffd0b50e177838] nfs_inode_set_delegation at ffffffffc1524a75 [nfsv4] 10 [ffffd0b50e177888] nfs4_process_delegation at ffffffffc14f41dd [nfsv4] 11 [ffffd0b50e1778a0] _nfs4_opendata_to_nfs4_state at ffffffffc1503edf [nfsv4] 12 [ffffd0b50e1778c0] _nfs4_open_and_get_state at ffffffffc1504e56 [nfsv4] 13 [ffffd0b50e177978] _nfs4_do_open at ffffffffc15051b8 [nfsv4] 14 [ffffd0b50e1779f8] nfs4_do_open at ffffffffc150559c [nfsv4] 15 [ffffd0b50e177a80] nfs4_atomic_open at ffffffffc15057fb [nfsv4] 16 [ffffd0b50e177ad0] nfs4_file_open at ffffffffc15219be [nfsv4] 17 [ffffd0b50e177b78] do_dentry_open at ffffffff9c09e6ea 18 [ffffd0b50e177ba8] vfs_open at ffffffff9c0a082e 19 [ffffd0b50e177bd0] dentry_open at ffffffff9c0a0935 The issue is that the delegreturn is being asked to wait for a layout return that cannot complete because a state recovery was initiated. The state recovery cannot complete until the open() finishes processing the delegations it was given. The solution is to propagate the existing flags that indicate a non-blocking call to the function pnfs_roc(), so that it knows not to wait in this situation.	N/A	More Details
CVE-2026-23077	In the Linux kernel, the following vulnerability has been resolved: mm/vma: fix anon_vma UAF on mremap() faulted, unfaulted merge Patch series "mm/vma: fix anon_vma UAF on mremap() faulted, unfaulted merge", v2. Commit 879bca0a2c4f ("mm/vma: fix incorrectly disallowed anonymous VMA merges") introduced the ability to merge previously unavailable VMA merge scenarios. However, it is handling merges incorrectly when it comes to mremap() of a faulted VMA adjacent to an unfaulted VMA. The issues arise in three cases: 1. Previous VMA unfaulted: copied -----| v |----------|.....| | unfaulted |(faulted VMA)| |----------|.....| prev 2. Next VMA unfaulted: copied -----| v |.....|----------| |(faulted VMA)| unfaulted | |.....|----------| next 3. Both adjacent VMAs unfaulted: copied -----| v |----------|.....|----------| | unfaulted |(faulted VMA)| unfaulted | |----------|.....|----------| prev next This series fixes each of these cases, and introduces self tests to assert that the issues are corrected. I also test a further case which was already handled, to assert that my changes continues to correctly handle it: 4. prev unfaulted, next faulted: copied -----| v |----------|.....|----------| | unfaulted |(faulted VMA)| faulted | |----------|.....|----------| prev next This bug was discovered via a syzbot report, linked to in the first patch in the series, I confirmed that this series fixes the bug. I also discovered that we are failing to check that the faulted VMA was not forked when merging a copied VMA in cases 1-3 above, an issue this series also addresses. I also added self tests to assert that this is resolved (and confirmed that the tests failed prior to this). I also cleaned up vma_expand() as part of this work, renamed vma_had_uncowed_parents() to vma_is_fork_child() as the previous name was unduly confusing, and simplified the comments around this function. This patch (of 4): Commit 879bca0a2c4f ("mm/vma: fix incorrectly disallowed anonymous VMA merges") introduced the ability to merge previously unavailable VMA merge scenarios. The key piece of logic introduced was the ability to merge a faulted VMA immediately next to an unfaulted VMA, which relies upon dup_anon_vma() to correctly handle anon_vma state. In the case of the merge of an existing VMA (that is changing properties of a VMA and then merging if those properties are shared by adjacent VMAs), dup_anon_vma() is invoked correctly. However in the case of the merge of a new VMA, a corner case peculiar to mremap() was missed. The issue is that vma_expand() only performs dup_anon_vma() if the target (the VMA that will ultimately become the merged VMA): is not the next VMA, i.e. the one that appears after the range in which the new VMA is to be established. A key insight here is that in all other cases other than mremap(), a new VMA merge either expands an existing VMA, meaning that the target VMA will be that VMA, or would have anon_vma be NULL. Specifically: * __mmap_region() - no anon_vma in place, initial mapping. * do_brk_flags() -	N/A	More Details

	expanding an existing VMA. * vma_merge_extend() - expanding an existing VMA. * relocate_vma_down() - no anon_vma in place, initial mapping. In addition, we are in the unique situation of needing to duplicate anon_vma state from a VMA that is neither the previous or next VMA being merged with. dup_anon_vma() deals exclusively with the target=unfaulted, src=faulted case. This leaves four possibilities, in each case where the copied VMA is faulted: 1. Previous VMA unfaulted: copied -----| ---truncated---		
CVE-2026-23060	In the Linux kernel, the following vulnerability has been resolved: crypto: authencesn - reject too-short AAD (assoclen<8) to match ESP/ESN spec authencesn assumes an ESP/ESN-formatted AAD. When assoclen is shorter than the minimum expected length, crypto_authenc_esn_decrypt() can advance past the end of the destination scatterlist and trigger a NULL pointer dereference in scatterwalk_map_and_copy(), leading to a kernel panic (DoS). Add a minimum AAD length check to fail fast on invalid inputs.	N/A	More Details
CVE-2026-23059	In the Linux kernel, the following vulnerability has been resolved: scsi: qla2xxx: Sanitize payload size to prevent member overflow In qla27xx_copy_fpin_pkt() and qla27xx_copy_multiple_pkt(), the frame_size reported by firmware is used to calculate the copy length into item->iocb. However, the iocb member is defined as a fixed-size 64-byte array within struct purex_item. If the reported frame_size exceeds 64 bytes, subsequent memcpy calls will overflow the iocb member boundary. While extra memory might be allocated, this cross-member write is unsafe and triggers warnings under CONFIG_FORTIFY_SOURCE. Fix this by capping total_bytes to the size of the iocb member (64 bytes) before allocation and copying. This ensures all copies remain within the bounds of the destination structure member.	N/A	More Details
CVE-2026-23057	In the Linux kernel, the following vulnerability has been resolved: vsock/virtio: Coalesce only linear skb vsock/virtio common tries to coalesce buffers in rx queue: if a linear skb (with a spare tail room) is followed by a small skb (length limited by GOOD_COPY_LEN = 128), an attempt is made to join them. Since the introduction of MSG_ZEROCOPY support, assumption that a small skb will always be linear is incorrect. In the zerocopy case, data is lost and the linear skb is appended with uninitialized kernel memory. Of all 3 supported virtio-based transports, only loopback-transport is affected. G2H virtio-transport rx queue operates on explicitly linear skbs; see virtio_vsock_alloc_linear_skb() in virtio_vsock_rx_fill(). H2G vhost-transport may allocate non-linear skbs, but only for sizes that are not considered for coalescence; see PAGE_ALLOC_COSTLY_ORDER in virtio_vsock_alloc_skb(). Ensure only linear skbs are coalesced. Note that skb_tailroom(last_skb) > 0 guarantees last_skb is linear.	N/A	More Details
CVE-2026-25843	Rejected reason: Not used	N/A	More Details
CVE-2025-71199	In the Linux kernel, the following vulnerability has been resolved: iio: adc: at91-sama5d2_adc: Fix potential use-after-free in sama5d2_adc driver at91_adc_interrupt can call at91_adc_touch_data_handler function to start the work by schedule_work(&st->touch_st.workq). If we remove the module which will call at91_adc_remove to make cleanup, it will free indio_dev through iio_device_unregister but quite a bit later. While the work mentioned above will be used. The sequence of operations that may lead to a UAF bug is as follows: CPU0 CPU1 | at91_adc_workq_handler at91_adc_remove | iio_device_unregister(indio_dev) | //free indio_dev a bit later | | iio_push_to_buffers(indio_dev) | //use indio_dev Fix it by ensuring that the work is canceled before proceeding with the cleanup in at91_adc_remove.	N/A	More Details
CVE-2025-29939	Improper access control in secure encrypted virtualization (SEV) could allow a privileged attacker to write to the reverse map page (RMP) during secure nested paging (SNP) initialization, potentially resulting in a loss of guest memory confidentiality and integrity.	N/A	More Details
CVE-2025-0029	Improper handling of error condition during host-induced faults can allow a local high-privileged attack to selectively drop guest DMA writes, potentially resulting in a loss of SEV-SNP guest memory integrity	N/A	More Details
CVE-2025-0012	Improper handling of overlap between the segmented reverse map table (RMP) and system management mode (SMM) memory could allow a privileged attacker corrupt or partially infer SMM memory resulting in loss of integrity or confidentiality.	N/A	More Details

CVE-2024-36355	Improper input validation in the SMM handler could allow an attacker with Ring0 access to write to SMRAM and modify execution flow for S3 (sleep) wake up, potentially resulting in arbitrary code execution.	N/A	More Details
CVE-2024-36311	A Time-of-check time-of-use (TOCTOU) race condition in the SMM communications buffer could allow a privileged attacker to bypass input validation and perform an out of bounds read or write, potentially resulting in loss of confidentiality, integrity, or availability.	N/A	More Details
CVE-2024-36310	Improper input validation in the SMM communications buffer could allow a privileged attacker to perform an out of bounds read or write to SMRAM potentially resulting in loss of confidentiality or integrity.	N/A	More Details
CVE-2024-21953	Improper input validation in IOMMU could allow a malicious hypervisor to reconfigure IOMMU registers resulting in loss of guest data integrity.	N/A	More Details
CVE-2021-26410	Improper syscall input validation in ASP (AMD Secure Processor) may force the kernel into reading syscall parameter values from its own memory space allowing an attacker to infer the contents of the kernel memory leading to potential information disclosure.	N/A	More Details
CVE-2021-26381	Improper system call parameter validation in the Trusted OS may allow a malicious driver to perform mapping or unmapping operations on a large number of pages, potentially resulting in kernel memory corruption.	N/A	More Details
CVE-2026-20984	Improper handling of insufficient permission in Galaxy Wearable installed on non-Samsung Device prior to version 2.2.68 allows local attackers to access sensitive information.	N/A	More Details
CVE-2026-25763	OpenProject is an open-source, web-based project management software. Prior to versions 16.6.7 and 17.0.3, an arbitrary file write vulnerability exists in OpenProject’s repository changes endpoint (/projects/:project_id/repository/changes) when rendering the “latest changes” view via git log. By supplying a specially crafted rev value (for example, rev=--output=/tmp/poc.txt), an attacker can inject git log command-line options. When OpenProject executes the SCM command, Git interprets the attacker-controlled rev as an option and writes the output to an attacker-chosen path. As a result, any user with the :browse_repository permission on the project can create or overwrite arbitrary files that the OpenProject process user is permitted to write. The written contents consist of git log output, but by crafting custom commits the attacker can still upload valid shell scripts, ultimately leading to RCE. The RCE lets the attacker create a reverse shell to the target host and view confidential files outside of OpenProject, such as /etc/passwd. This issue has been patched in versions 16.6.7 and 17.0.3.	N/A	More Details
CVE-2026-20985	Improper input validation in Samsung Members prior to version 5.6.00.11 allows remote attackers to connect arbitrary URL and launch arbitrary activity with Samsung Members privilege. User interaction is required for triggering this vulnerability.	N/A	More Details
CVE-2026-25758	Spree is an open source e-commerce solution built with Ruby on Rails. A critical IDOR vulnerability exists in Spree Commerce's guest checkout flow that allows any guest user to bind arbitrary guest addresses to their order by manipulating address ID parameters. This enables unauthorized access to other guests' personally identifiable information (PII) including names, addresses and phone numbers. The vulnerability bypasses existing ownership validation checks and affects all guest checkout transactions. This vulnerability is fixed in 4.10.3, 5.0.8, 5.1.10, 5.2.7, and 5.3.2.	N/A	More Details
CVE-2026-25533	Enclave is a secure JavaScript sandbox designed for safe AI agent code execution. Prior to 2.10.1, the existing layers of security in enclave-vm are insufficient: The AST sanitization can be bypassed with dynamic property accesses, the hardening of the error objects does not cover the peculiar behavior or the vm module and the function constructor access prevention can be side-stepped by leveraging host object references. This vulnerability is fixed in 2.10.1.	N/A	More Details
CVE-2026-20986	Path traversal in Samsung Members prior to Chinese version 15.5.05.4 allows local attackers to overwrite data within Samsung Members.	N/A	More Details

CVE-2026-20987	Improper input validation in GalaxyDiagnostics prior to version 3.5.050 allows local privileged attackers to execute privileged commands.	N/A	More Details
CVE-2026-21393	Movable Type contains a stored cross-site scripting vulnerability in Edit Comment. If crafted input is stored by an attacker, arbitrary script may be executed on a logged-in user's web browser. Note that Movable Type 7 series and 8.4 series, which are End-of-Life (EOL), are affected by the vulnerability as well.	N/A	More Details
CVE-2026-22875	Movable Type contains a stored cross-site scripting vulnerability in Export Sites. If crafted input is stored by an attacker, arbitrary script may be executed on a logged-in user's web browser. Note that Movable Type 7 series and 8.4 series, which are End-of-Life (EOL), are affected by the vulnerability as well.	N/A	More Details
CVE-2025-0031	A use after free in the SEV firmware could allow a malicous hypervisor to activate a migrated guest with the SINGLE_SOCKET policy on a different socket than the migration agent potentially resulting in loss of integrity.	N/A	More Details
CVE-2025-29946	Insufficient or Incomplete Data Removal in Hardware Component in SEV firmware doesn't fully flush IOMMU. This can potentially lead to a loss of confidentiality and integrity in guest memory.	N/A	More Details
CVE-2025-71198	In the Linux kernel, the following vulnerability has been resolved: iio: imu: st_lsm6dsx: fix iio_chan_spec for sensors without event detection The st_lsm6dsx_acc_channels array of struct iio_chan_spec has a non-NULL event_spec field, indicating support for IIO events. However, event detection is not supported for all sensors, and if userspace tries to configure accelerometer wakeup events on a sensor device that does not support them (e.g. LSM6DS0), st_lsm6dsx_write_event() dereferences a NULL pointer when trying to write to the wakeup register. Define an additional struct iio_chan_spec array whose members have a NULL event_spec field, and use this array instead of st_lsm6dsx_acc_channels for sensors without event detection capability.	N/A	More Details
CVE-2025-29948	Improper access control in AMD Secure Encrypted Virtualization (SEV) firmware could allow a malicious hypervisor to bypass RMP protections, potentially resulting in a loss of SEV-SNP guest memory integrity.	N/A	More Details
CVE-2026-25251	Rejected reason: This has been moved to the REJECTED state because the information source is under review. If circumstances change, it is possible that this will be moved to the PUBLISHED state at a later date.	N/A	More Details
CVE-2026-26007	cryptography is a package designed to expose cryptographic primitives and recipes to Python developers. Prior to 46.0.5, the public_key_from_numbers (or EllipticCurvePublicNumbers.public_key()), EllipticCurvePublicNumbers.public_key(), load_der_public_key() and load_pem_public_key() functions do not verify that the point belongs to the expected prime-order subgroup of the curve. This missing validation allows an attacker to provide a public key point P from a small-order subgroup. This can lead to security issues in various situations, such as the most commonly used signature verification (ECDSA) and shared key negotiation (ECDH). When the victim computes the shared secret as S = [victim_private_key]P via ECDH, this leaks information about victim_private_key mod (small_subgroup_order). For curves with cofactor > 1, this reveals the least significant bits of the private key. When these weak public keys are used in ECDSA , it's easy to forge signatures on the small subgroup. Only SECT curves are impacted by this. This vulnerability is fixed in 46.0.5.	N/A	More Details
CVE-2025-69621	An arbitrary file overwrite vulnerability in the file import process of Comic Book Reader v1.0.95 allows attackers to overwrite critical internal files, potentially leading to arbitrary code execution or exposure of sensitive information.	N/A	More Details
CVE-2025-29867	Access of Resource Using Incompatible Type ('Type Confusion') vulnerability in Hancom Inc. Hancom Office 2018, Hancom Inc. Hancom Office 2020, Hancom Inc. Hancom Office 2022, Hancom Inc. Hancom Office 2024 allows File Content Injection.This issue affects Hancom Office 2018: before 10.0.0.12681; Hancom Office 2020: before 11.0.0.8916; Hancom Office 2022: before 12.0.0.4426; Hancom Office 2024: before 13.0.0.3050.	N/A	More Details

CVE-2026-25757	Spree is an open source e-commerce solution built with Ruby on Rails. Prior to versions 5.0.8, 5.1.10, 5.2.7, and 5.3.2, unauthenticated users can view completed guest orders by Order ID. This issue may lead to disclosure of PII of guest users (including names, addresses and phone numbers). This issue has been patched in versions 5.0.8, 5.1.10, 5.2.7, and 5.3.2.	N/A	More Details
CVE-2023-6763	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2025-54514	Improper isolation of shared resources on a system on a chip by a malicious local attacker with high privileges could potentially lead to a partial loss of integrity.	N/A	More Details
CVE-2025-52536	Improper Prevention of Lock Bit Modification in SEV firmware could allow a privileged attacker to downgrade firmware potentially resulting in a loss of integrity.	N/A	More Details
CVE-2025-52534	Improper bound check within AMD CPU microcode can allow a malicious guest to write to host memory, potentially resulting in loss of integrity.	N/A	More Details
CVE-2025-48517	Insufficient Granularity of Access Control in SEV firmware could allow a privileged user with a malicious hypervisor to create a SEV-ES guest with an ASID in the range meant for SEV-SNP guests potentially resulting in a partial loss of confidentiality.	N/A	More Details
CVE-2025-48515	Insufficient parameter sanitization in AMD Secure Processor (ASP) Boot Loader could allow an attacker with access to SPIROM upgrade to overwrite the memory, potentially resulting in arbitrary code execution.	N/A	More Details
CVE-2025-48514	Insufficient Granularity of Access Control in SEV firmware can allow a privileged attacker to create a SEV-ES Guest to attack SNP guest, potentially resulting in a loss of confidentiality.	N/A	More Details
CVE-2025-48509	Missing Checks in certain functions related to RMP initialization can allow a local admin privileged attacker to cause misidentification of I/O memory, potentially resulting in a loss of guest memory integrity	N/A	More Details
CVE-2025-29952	Improper Initialization within the AMD Secure Encrypted Virtualization (SEV) firmware can allow an admin privileged attacker to corrupt RMP covered memory, potentially resulting in loss of guest memory integrity	N/A	More Details
CVE-2025-29951	A buffer overflow in the AMD Secure Processor (ASP) bootloader could allow an attacker to overwrite memory, potentially resulting in privilege escalation and arbitrary code execution.	N/A	More Details
CVE-2025-29950	Improper input validation in system management mode (SMM) could allow a privileged attacker to overwrite stack memory leading to arbitrary code execution.	N/A	More Details
CVE-2025-29949	Insufficient input parameter sanitization in AMD Secure Processor (ASP) Boot Loader (legacy recovery mode only) could allow an attacker to write out-of-bounds to corrupt Secure DRAM potentially resulting in denial of service.	N/A	More Details
CVE-2026-23704	A non-administrative user can upload malicious files. When an administrator or the product accesses that file, an arbitrary script may be executed on the administrator's browser. Note that Movable Type 7 series and 8.4 series, which are End-of-Life (EOL), are affected by the vulnerability as well.	N/A	More Details
CVE-2026-24447	If a malformed data is input to the affected product, a CSV file downloaded from the affected product may contain such malformed data. When a victim user download and open such a CSV file, the embedded code may be executed in the user's environment. Note that Movable Type 7 series and 8.4 series, which are End-of-Life (EOL), are affected by the vulnerability as well.	N/A	More Details
	BeyondTrust Remote Support (RS) and certain older versions of Privileged Remote Access		

CVE-2026-1731	(PRA) contain a critical pre-authentication remote code execution vulnerability. By sending specially crafted requests, an unauthenticated remote attacker may be able to execute operating system commands in the context of the site user.	N/A	More Details
CVE-2026-1727	The Agentspace service was affected by a vulnerability that exposed sensitive information due to the use of predictable Google Cloud Storage bucket names. These names were utilized for error logs and temporary staging during data imports from GCS and Cloud SQL. This predictability allowed an attacker to engage in "bucket squatting" by establishing these buckets before a victim's initial use. All versions after December 12th, 2025 have been updated to protect from this vulnerability. No user action is required for this.	N/A	More Details
CVE-2026-23041	In the Linux kernel, the following vulnerability has been resolved: bnxt_en: Fix NULL pointer crash in bnxt_ptp_enable during error cleanup When bnxt_init_one() fails during initialization (e.g., bnxt_init_int_mode returns -ENODEV), the error path calls bnxt_free_hwrm_resources() which destroys the DMA pool and sets bp->hwrm_dma_pool to NULL. Subsequently, bnxt_ptp_clear() is called, which invokes ptp_clock_unregister(). Since commit a60fc3294a37 ("ptp: rework ptp_clock_unregister() to disable events"), ptp_clock_unregister() now calls ptp_disable_all_events(), which in turn invokes the driver's .enable() callback (bnxt_ptp_enable()) to disable PTP events before completing the unregistration. bnxt_ptp_enable() attempts to send HWRM commands via bnxt_ptp_cfg_pin() and bnxt_ptp_cfg_event(), both of which call hwrm_req_init(). This function tries to allocate from bp->hwrm_dma_pool, causing a NULL pointer dereference: bnxt_en 0000:01:00.0 (unnamed net_device) (uninitialized): bnxt_init_int_mode err: ffffffed KASAN: null-ptr-deref in range [0x0000000000000028-0x000000000000002f] Call Trace: __hwrm_req_init (drivers/net/ethernet/broadcom/bnxt/bnxt_hwrm.c:72) bnxt_ptp_enable (drivers/net/ethernet/broadcom/bnxt/bnxt_ptp.c:323 drivers/net/ethernet/broadcom/bnxt/bnxt_ptp.c:517) ptp_disable_all_events (drivers/ptp/ptp_chardev.c:66) ptp_clock_unregister (drivers/ptp/ptp_clock.c:518) bnxt_ptp_clear (drivers/net/ethernet/broadcom/bnxt/bnxt_ptp.c:1134) bnxt_init_one (drivers/net/ethernet/broadcom/bnxt/bnxt.c:16889) Lines are against commit f8f9c1f4d0c7 ("Linux 6.19-rc3") Fix this by clearing and unregistering ptp (bnxt_ptp_clear()) before freeing HWRM resources.	N/A	More Details
CVE-2026-23042	In the Linux kernel, the following vulnerability has been resolved: idpf: fix aux device unplugging when rdma is not supported by vport If vport flags do not contain VIRTCHNL2_VPORT_ENABLE_RDMA, driver does not allocate vdev_info for this vport. This leads to kernel NULL pointer dereference in idpf_idc_vport_dev_down(), which references vdev_info for every vport regardless. Check, if vdev_info was ever allocated before unplugging aux device.	N/A	More Details
CVE-2026-23043	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix NULL pointer dereference in do_abort_log_replay() Coverity reported a NULL pointer dereference issue (CID 1666756) in do_abort_log_replay(). When btrfs_alloc_path() fails in replay_one_buffer(), wc->subvol_path is NULL, but btrfs_abort_log_replay() calls do_abort_log_replay() which unconditionally dereferences wc->subvol_path when attempting to print debug information. Fix this by adding a NULL check before dereferencing wc->subvol_path in do_abort_log_replay().	N/A	More Details
CVE-2026-23044	In the Linux kernel, the following vulnerability has been resolved: PM: hibernate: Fix crash when freeing invalid crypto compressor When crypto_alloc_acomp() fails, it returns an ERR_PTR value, not NULL. The cleanup code in save_compressed_image() and load_compressed_image() unconditionally calls crypto_free_acomp() without checking for ERR_PTR, which causes crypto_acomp_tfm() to dereference an invalid pointer and crash the kernel. This can be triggered when the compression algorithm is unavailable (e.g., CONFIG_CRYPTO_LZO not enabled). Fix by adding IS_ERR_OR_NULL() checks before calling crypto_free_acomp() and acomp_request_free(), similar to the existing kthread_stop() check. [rjw: Added 2 empty code lines]	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: net/ena: fix missing lock when update devlink params Fix assert lock warning while calling devl_param_driverinit_value_set() in ena. WARNING: net/devlink/core.c:261 at devl_assert_locked+0x62/0x90, CPU#0: kworker/0:0/9 CPU: 0 UID: 0 PID: 9 Comm:		

CVE-2026-23045	kworker/0:0 Not tainted 6.19.0-rc2+ #1 PREEMPT(lazy) Hardware name: Amazon EC2 m8i-flex.4xlarge/, BIOS 1.0 10/16/2017 Workqueue: events work_for_cpu_fn RIP: 0010:devl_assert_locked+0x62/0x90 Call Trace: <TASK> devl_param_driverinit_value_set+0x15/0x1c0 ena_devlink_alloc+0x18c/0x220 [ena] ? __pfx_ena_devlink_alloc+0x10/0x10 [ena] ? trace_hardirqs_on+0x18/0x140 ? lockdep_hardirqs_on+0x8c/0x130 ? __raw_spin_unlock_irqrestore+0x5d/0x80 ? __raw_spin_unlock_irqrestore+0x46/0x80 ? devm_ioremap_wc+0x9a/0xd0 ena_probe+0x4d2/0x1b20 [ena] ? __lock_acquire+0x56a/0xbd0 ? __pfx_ena_probe+0x10/0x10 [ena] ? local_clock+0x15/0x30 ? __lock_release.isra.0+0x1c9/0x340 ? mark_held_locks+0x40/0x70 ? lockdep_hardirqs_on_prepare.part.0+0x92/0x170 ? trace_hardirqs_on+0x18/0x140 ? lockdep_hardirqs_on+0x8c/0x130 ? __raw_spin_unlock_irqrestore+0x5d/0x80 ? __raw_spin_unlock_irqrestore+0x46/0x80 ? __pfx_ena_probe+0x10/0x10 [ena] ..... </TASK>	N/A	More Details
CVE-2026-23046	In the Linux kernel, the following vulnerability has been resolved: virtio_net: fix device mismatch in devm_kzalloc/devm_kfree Initial rss_hdr allocation uses virtio_device->device, but virtnet_set_queues() frees using net_device->device. This device mismatch causing below devres warning [3788.514041] ------------[cut here]------------ [3788.514044] WARNING: drivers/base/devres.c:1095 at devm_kfree+0x84/0x98, CPU#16: vdpa/1463 [3788.514054] Modules linked in: octep_vdpa virtio_net virtio_vdpa [last unloaded: virtio_vdpa] [3788.514064] CPU: 16 UID: 0 PID: 1463 Comm: vdpa Tainted: G W 6.18.0 #10 PREEMPT [3788.514067] Tainted: [W]=WARN [3788.514069] Hardware name: Marvell CN106XX board (DT) [3788.514071] pstate: 63400009 (nZCv daif +PAN -UAO +TCO +DIT -SSBS BTYPE=--) [3788.514074] pc : devm_kfree+0x84/0x98 [3788.514076] lr : devm_kfree+0x54/0x98 [3788.514079] sp : ffff800084e2f220 [3788.514080] x29: ffff800084e2f220 x28: ffff0003b2366000 x27: 000000000000003f [3788.514085] x26: 000000000000003f x25: ffff000106f17c10 x24: 0000000000000080 [3788.514089] x23: ffff00045bb8ab08 x22: ffff00045bb8a000 x21: 0000000000000018 [3788.514093] x20: ffff0004355c3080 x19: ffff00045bb8aa00 x18: 0000000000080000 [3788.514098] x17: 0000000000000040 x16: 000000000000001f x15: 000000000007ffff [3788.514102] x14: 0000000000000488 x13: 0000000000000005 x12: 00000000000fffff [3788.514106] x11: ffffffffffffffff x10: 0000000000000005 x9 : ffff800080c8c05c [3788.514110] x8 : ffff800084e2eeb8 x7 : 0000000000000000 x6 : 000000000000003f [3788.514115] x5 : ffff8000831bafe0 x4 : ffff800080c8b010 x3 : ffff0004355c3080 [3788.514119] x2 : ffff0004355c3080 x1 : 0000000000000000 x0 : 0000000000000000 [3788.514123] Call trace: [3788.514125] devm_kfree+0x84/0x98 (P) [3788.514129] virtnet_set_queues+0x134/0x2e8 [virtio_net] [3788.514135] virtnet_probe+0x9c0/0xe00 [virtio_net] [3788.514139] virtio_dev_probe+0x1e0/0x338 [3788.514144] really_probe+0xc8/0x3a0 [3788.514149] __driver_probe_device+0x84/0x170 [3788.514152] driver_probe_device+0x44/0x120 [3788.514155] __device_attach_driver+0xc4/0x168 [3788.514158] bus_for_each_drv+0x8c/0xf0 [3788.514161] __device_attach+0xa4/0x1c0 [3788.514164] device_initial_probe+0x1c/0x30 [3788.514168] bus_probe_device+0xb4/0xc0 [3788.514170] device_add+0x614/0x828 [3788.514173] register_virtio_device+0x214/0x258 [3788.514175] virtio_vdpa_probe+0xa0/0x110 [virtio_vdpa] [3788.514179] vdpa_dev_probe+0xa8/0xd8 [3788.514183] really_probe+0xc8/0x3a0 [3788.514186] __driver_probe_device+0x84/0x170 [3788.514189] driver_probe_device+0x44/0x120 [3788.514192] __device_attach_driver+0xc4/0x168 [3788.514195] bus_for_each_drv+0x8c/0xf0 [3788.514197] __device_attach+0xa4/0x1c0 [3788.514200] device_initial_probe+0x1c/0x30 [3788.514203] bus_probe_device+0xb4/0xc0 [3788.514206] device_add+0x614/0x828 [3788.514209] _vdpa_register_device+0x58/0x88 [3788.514211] octep_vdpa_dev_add+0x104/0x228 [octep_vdpa] [3788.514215] vdpa_nl_cmd_dev_add_set_doit+0x2d0/0x3c0 [3788.514218] genl_family_rcv_msg_doit+0xe4/0x158 [3788.514222] genl_rcv_msg+0x218/0x298 [3788.514225] netlink_rcv_skb+0x64/0x138 [3788.514229] genl_rcv+0x40/0x60 [3788.514233] netlink_unicast+0x32c/0x3b0 [3788.514237] netlink_sendmsg+0x170/0x3b8 [3788.514241] __sys_sendto+0x12c/0x1c0 [3788.514246] __arm64_sys_sendto+0x30/0x48 [3788.514249] invoke_syscall.constprop.0+0x58/0xf8 [3788.514255] do_el0_svc+0x48/0xd0 [3788.514259] el0_svc+0x48/0x210 [3788.514264] el0t_64_sync_handler+0xa0/0xe8 [3788.514268] el0t_64_sync+0x198/0x1a0 [3788.514271] ---[end trace 0000000000000000]--- Fix by using virtio_device->device consistently for allocation and deallocation	N/A	More Details

CVE-2026-23047	In the Linux kernel, the following vulnerability has been resolved: libceph: make calc_target() set t->paused, not just clear it Currently calc_target() clears t->paused if the request shouldn't be paused anymore, but doesn't ever set t->paused even though it's able to determine when the request should be paused. Setting t->paused is left to __submit_request() which is fine for regular requests but doesn't work for linger requests -- since __submit_request() doesn't operate on linger requests, there is nowhere for lreq->t.paused to be set. One consequence of this is that watches don't get reestablished on paused -> unpaused transitions in cases where requests have been paused long enough for the (paused) unwatch request to time out and for the subsequent (re)watch request to enter the paused state. On top of the watch not getting reestablished, rbd_reregister_watch() gets stuck with rbd_dev->watch_mutex held: rbd_register_watch __rbd_register_watch ceph_osdc_watch linger_reg_commit_wait It's waiting for lreq->reg_commit_wait to be completed, but for that to happen the respective request needs to end up on need_resend_linger list and be kicked when requests are unpaused. There is no chance for that if the request in question is never marked paused in the first place. The fact that rbd_dev->watch_mutex remains taken out forever then prevents the image from getting unmapped -- "rbd unmap" would inevitably hang in D state on an attempt to grab the mutex.	N/A	More Details
CVE-2026-23048	In the Linux kernel, the following vulnerability has been resolved: udp: call skb_orphan() before skb_attempt_defer_free() Standard UDP receive path does not use skb->destructor. But skmsg layer does use it, since it calls skb_set_owner_sk_safe() from udp_read_skb(). This then triggers this warning in skb_attempt_defer_free(): DEBUG_NET_WARN_ON_ONCE(skb->destructor); We must call skb_orphan() to fix this issue.	N/A	More Details
CVE-2026-25844	Rejected reason: Not used	N/A	More Details
CVE-2025-71193	In the Linux kernel, the following vulnerability has been resolved: phy: qcom-qusb2: Fix NULL pointer dereference on early suspend Enabling runtime PM before attaching the QPHY instance as driver data can lead to a NULL pointer dereference in runtime PM callbacks that expect valid driver data. There is a small window where the suspend callback may run after PM runtime enabling and before runtime forbid. This causes a sporadic crash during boot: ``` Unable to handle kernel NULL pointer dereference at virtual address 00000000000000a1 [...] CPU: 0 UID: 0 PID: 11 Comm: kworker/0:1 Not tainted 6.16.7+ #116 PREEMPT Workqueue: pm pm_runtime_work pstate: 20000005 (nzCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : qusb2_phy_runtime_suspend+0x14/0x1e0 [phy_qcom_qusb2] lr : pm_generic_runtime_suspend+0x2c/0x44 [...] ``` Attach the QPHY instance as driver data before enabling runtime PM to prevent NULL pointer dereference in runtime PM callbacks. Reorder pm_runtime_enable() and pm_runtime_forbid() to prevent a short window where an unnecessary runtime suspend can occur. Use the devres-managed version to ensure PM runtime is symmetrically disabled during driver removal for proper cleanup.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix deadlock in wait_current_trans() due to ignored transaction type When wait_current_trans() is called during start_transaction(), it currently waits for a blocked transaction without considering whether the given transaction type actually needs to wait for that particular transaction state. The btrfs_blocked_trans_types[] array already defines which transaction types should wait for which transaction states, but this check was missing in wait_current_trans(). This can lead to a deadlock scenario involving two transactions and pending ordered extents: 1. Transaction A is in TRANS_STATE_COMMIT_DOING state 2. A worker processing an ordered extent calls start_transaction() with TRANS_JOIN 3. join_transaction() returns -EBUSY because Transaction A is in TRANS_STATE_COMMIT_DOING 4. Transaction A moves to TRANS_STATE_UNBLOCKED and completes 5. A new Transaction B is created (TRANS_STATE_RUNNING) 6. The ordered extent from step 2 is added to Transaction B's pending ordered extents 7. Transaction B immediately starts commit by another task and enters TRANS_STATE_COMMIT_START 8. The worker finally reaches wait_current_trans(), sees Transaction B in TRANS_STATE_COMMIT_START (a blocked state), and waits unconditionally 9. However, TRANS_JOIN should NOT wait for TRANS_STATE_COMMIT_START according to btrfs_blocked_trans_types[] 10. Transaction B is waiting for pending ordered extents to complete 11. Deadlock: Transaction B waits for ordered extent, ordered extent		

CVE-2025-71194	waits for Transaction B This can be illustrated by the following call stacks: CPU0 CPU1 btrfs_finish_ordered_io() start_transaction(TRANS_JOIN) join_transaction() # -EBUSY (Transaction A is # TRANS_STATE_COMMIT_DOING) # Transaction A completes # Transaction B created # ordered extent added to # Transaction B's pending list btrfs_commit_transaction() # Transaction B enters # TRANS_STATE_COMMIT_START # waiting for pending ordered # extents wait_current_trans() # waits for Transaction B # (should not wait!) Task bstore_kv_sync in btrfs_commit_transaction waiting for ordered extents: __schedule+0x2e7/0x8a0 schedule+0x64/0xe0 btrfs_commit_transaction+0xbf7/0xda0 [btrfs] btrfs_sync_file+0x342/0x4d0 [btrfs] __x64_sys_fdatasync+0x4b/0x80 do_syscall_64+0x33/0x40 entry_SYSCALL_64_after_hwframe+0x44/0xa9 Task kworker in wait_current_trans waiting for transaction commit: Workqueue: btrfs-syno_nocow btrfs_work_helper [btrfs] __schedule+0x2e7/0x8a0 schedule+0x64/0xe0 wait_current_trans+0xb0/0x110 [btrfs] start_transaction+0x346/0x5b0 [btrfs] btrfs_finish_ordered_io.isra.0+0x49b/0x9c0 [btrfs] btrfs_work_helper+0xe8/0x350 [btrfs] process_one_work+0x1d3/0x3c0 worker_thread+0x4d/0x3e0 kthread+0x12d/0x150 ret_from_fork+0x1f/0x30 Fix this by passing the transaction type to wait_current_trans() and checking btrfs_blocked_trans_types[cur_trans->state] against the given type before deciding to wait. This ensures that transaction types which are allowed to join during certain blocked states will not unnecessarily wait and cause deadlocks.	N/A	More Details
CVE-2026-25845	Rejected reason: Not used	N/A	More Details
CVE-2026-25631	n8n is an open source workflow automation platform. Prior to 1.121.0, there is a vulnerability in the HTTP Request node's credential domain validation allowed an authenticated attacker to send requests with credentials to unintended domains, potentially leading to credential exfiltration. This only might affect user who have credentials that use wildcard domain patterns (e.g., *.example.com) in the "Allowed domains" setting. This issue is fixed in version 1.121.0 and later.	N/A	More Details
CVE-2026-25727	time provides date and time handling in Rust. From 0.3.6 to before 0.3.47, when user-provided input is provided to any type that parses with the RFC 2822 format, a denial of service attack via stack exhaustion is possible. The attack relies on formally deprecated and rarely-used features that are part of the RFC 2822 format used in a malicious manner. Ordinary, non-malicious input will never encounter this scenario. A limit to the depth of recursion was added in v0.3.47. From this version, an error will be returned rather than exhausting the stack.	N/A	More Details
CVE-2025-71195	In the Linux kernel, the following vulnerability has been resolved: dmaengine: xilinx: xdma: Fix regmap max_register The max_register field is assigned the size of the register memory region instead of the offset of the last register. The result is that reading from the regmap via debugfs can cause a segmentation fault: tail /sys/kernel/debug/regmap/xdma.1.auto/registers Unable to handle kernel paging request at virtual address ffff800082f70000 Mem abort info: ESR = 0x0000000096000007 EC = 0x25: DABT (current EL), IL = 32 bits SET = 0, FnV = 0 EA = 0, S1PTW = 0 FSC = 0x07: level 3 translation fault [...] Call trace: regmap_mmio_read32le+0x10/0x30 _regmap_bus_reg_read+0x74/0xc0 _regmap_read+0x68/0x198 regmap_read+0x54/0x88 regmap_read_debugfs+0x140/0x380 regmap_map_read_file+0x30/0x48 full_proxy_read+0x68/0xc8 vfs_read+0xcc/0x310 ksys_read+0x7c/0x120 __arm64_sys_read+0x24/0x40 invoke_syscall.constprop.0+0x64/0x108 do_el0_svc+0xb0/0xd8 el0_svc+0x38/0x130 el0t_64_sync_handler+0x120/0x138 el0t_64_sync+0x194/0x198 Code: aa1e03e9 d503201f f9400000 8b214000 (b9400000) ---[end trace 0000000000000000]--- note: tail[1217] exited with irqs disabled note: tail[1217] exited with preempt_count 1 Segmentation fault	N/A	More Details
CVE-2025-71196	In the Linux kernel, the following vulnerability has been resolved: phy: stm32-usphyc: Fix off by one in probe() The "index" variable is used as an index into the usbphyc->phys[] array which has usbphyc->nphys elements. So if it is equal to usbphyc->nphys then it is one element out of bounds. The "index" comes from the device tree so it's data that we trust	N/A	More Details

	and it's unlikely to be wrong, however it's obviously still worth fixing the bug. Change the > to >=.		
CVE-2025-71197	In the Linux kernel, the following vulnerability has been resolved: w1: therm: Fix off-by-one buffer overflow in alarms_store The sysfs buffer passed to alarms_store() is allocated with 'size + 1' bytes and a NUL terminator is appended. However, the 'size' argument does not account for this extra byte. The original code then allocated 'size' bytes and used strcpy() to copy 'buf', which always writes one byte past the allocated buffer since strcpy() copies until the NUL terminator at index 'size'. Fix this by parsing the 'buf' parameter directly using simple_strtoll() without allocating any intermediate memory or string copying. This removes the overflow while simplifying the code.	N/A	More Details
CVE-2026-23040	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211_hwsim: fix typo in frequency notification The NAN notification is for 5745 MHz which corresponds to channel 149 and not 5475 which is not actually a valid channel. This could result in a NULL pointer dereference in cfg80211_next_nan_dw_notif.	N/A	More Details
CVE-2025-71192	In the Linux kernel, the following vulnerability has been resolved: ALSA: ac97: fix a double free in snd_ac97_controller_register() If ac97_add_adapter() fails, put_device() is the correct way to drop the device reference. kfree() is not required. Add kfree() if idr_alloc() fails and in ac97_adapter_release() to do the cleanup. Found by code review.	N/A	More Details
CVE-2026-23085	In the Linux kernel, the following vulnerability has been resolved: irqchip/gic-v3-its: Avoid truncating memory addresses On 32-bit machines with CONFIG_ARM_LPAE, it is possible for lowmem allocations to be backed by addresses physical memory above the 32-bit address limit, as found while experimenting with larger VMSPLIT configurations. This caused the qemu virt model to crash in the GICv3 driver, which allocates the 'itt' object using GFP_KERNEL. Since all memory below the 4GB physical address limit is in ZONE_DMA in this configuration, kmalloc() defaults to higher addresses for ZONE_NORMAL, and the ITS driver stores the physical address in a 32-bit 'unsigned long' variable. Change the itt_addr variable to the correct phys_addr_t type instead, along with all other variables in this driver that hold a physical address. The gicv5 driver correctly uses u64 variables, while all other irqchip drivers don't call virt_to_phys or similar interfaces. It's expected that other device drivers have similar issues, but fixing this one is sufficient for booting a virtio based guest.	N/A	More Details
CVE-2026-25646	LIBPNG is a reference library for use in applications that read, create, and manipulate PNG (Portable Network Graphics) raster image files. Prior to 1.6.55, an out-of-bounds read vulnerability exists in the png_set_quantize() API function. When the function is called with no histogram and the number of colors in the palette is more than twice the maximum supported by the user's display, certain palettes will cause the function to enter into an infinite loop that reads past the end of an internal heap-allocated buffer. The images that trigger this vulnerability are valid per the PNG specification. This vulnerability is fixed in 1.6.55.	N/A	More Details
CVE-2026-25729	DeepAudit is a multi-agent system for code vulnerability discovery. In 3.0.4 and earlier, there is an improper access control vulnerability in the /api/v1/users/ endpoint allows any authenticated user to enumerate all users in the system and retrieve sensitive information including email addresses, phone numbers, full names, and role information.	N/A	More Details
CVE-2026-25837	Rejected reason: Not used	N/A	More Details
CVE-2026-26003	FastGPT is an AI Agent building platform. From 4.14.0 to 4.14.5, attackers can directly access the plugin system through FastGPT/api/plugin/xxx without authentication, thereby threatening the plugin system. This may cause the plugin system to crash and the loss of plugin installation status, but it will not result in key leakage. For older versions, as there are only operation interfaces for obtaining information, the impact is almost negligible. This vulnerability is fixed in 4.14.5-fix.	N/A	More Details
CVE-	EverShop is a TypeScript-first eCommerce platform. During category update and deletion event handling, the application embeds path / request_path values—derived from the url_key stored in the database—into SQL statements via string concatenation and passes		More

2026-25993	them to execute(). As a result, if a malicious string is stored in url_key , subsequent event processing modifies and executes the SQL statement, leading to a second-order SQL injection. Patched from v2.1.1.	N/A	More Details
CVE-2026-25838	Rejected reason: Not used	N/A	More Details
CVE-2026-25950	Rejected reason: Further research determined the issue is not a vulnerability.	N/A	More Details
CVE-2026-25728	ClipBucket v5 is an open source video sharing platform. Prior to 5.5.3 - #40, a Time-of-Check to Time-of-Use (TOCTOU) race condition vulnerability exists in ClipBucket's avatar and background image upload functionality. The application moves uploaded files to a web-accessible location before validating them, creating a window where an attacker can execute arbitrary PHP code before the file is deleted. The uploaded file was moved to a web-accessible path via move_uploaded_file(), then validated via ValidateImage(). If validation failed, the file was deleted via @unlink(). This vulnerability is fixed in 5.5.3 - #40.	N/A	More Details
CVE-2025-41085	Stored Cross-Site Scripting (XSS) vulnerability type in Apidog in the version 2.7.15, where SVG image uploads are not properly sanitized. This allows attackers to embed malicious scripts in SVG files by sending a POST request to '/api/v1/user-avatar', which are then stored on the server and executed in the context of any user accessing the compromised resource.	N/A	More Details
CVE-2026-25842	Rejected reason: Not used	N/A	More Details
CVE-2026-1622	Neo4j Enterprise and Community editions versions prior to 2026.01.3 and 5.26.21 are vulnerable to a potential information disclosure by a user who has ability to access the local log files. The "obfuscate_literals" option in the query logs does not redact error information, exposing unredacted data in the query log when a customer writes a query that fails. It can allow a user with legitimate access to the local log files to obtain information they are not authorised to see. If this user is also in a position to run queries and trigger errors, this vulnerability can potentially help them to infer information they are not authorised to see through their intended database access. We recommend upgrading to versions 2026.01.3 (or 5.26.21) where the issue is fixed, and reviewing query log files permissions to ensure restricted access. If your configuration had db.logs.query.obfuscate_literals enabled, and you wish the obfuscation to cover the error messages as well, you need to enable the new configuration setting db.logs.query.obfuscate_errors once you have upgraded Neo4j.	N/A	More Details
CVE-2026-0873	On a Cryptobox platform where administrator segregation based on entities is used, some vulnerabilities in Ercom Cryptobox administration console allows an authenticated entity administrator with knowledge to elevate his account to global administrator.	N/A	More Details
CVE-2025-69618	An arbitrary file overwrite vulnerability in the file import process of Tarot, Astro & Healing v11.4.0 allows attackers to overwrite critical internal files, potentially leading to arbitrary code execution or exposure of sensitive information.	N/A	More Details
CVE-2025-70997	A vulnerability has been discovered in eladmin v2.7 and before. This vulnerability allows for an arbitrary user password reset under any user permission level.	N/A	More Details
CVE-2026-25839	Rejected reason: Not used	N/A	More Details
CVE-2026-25840	Rejected reason: Not used	N/A	More Details
CVE-2026-	Rejected reason: Not used	N/A	More

2026-25841	Rejected reason: Not used	N/A	Details
CVE-2026-23084	In the Linux kernel, the following vulnerability has been resolved: be2net: Fix NULL pointer dereference in be_cmd_get_mac_from_list When the parameter pmac_id_valid argument of be_cmd_get_mac_from_list() is set to false, the driver may request the PMAC_ID from the firmware of the network card, and this function will store that PMAC_ID at the provided address pmac_id. This is the contract of this function. However, there is a location within the driver where both pmac_id_valid == false and pmac_id == NULL are being passed. This could result in dereferencing a NULL pointer. To resolve this issue, it is necessary to pass the address of a stub variable to the function.	N/A	More Details
CVE-2025-64111	Gogs is an open source self-hosted Git service. In version 0.13.3 and prior, due to the insufficient patch for CVE-2024-56731, it's still possible to update files in the .git directory and achieve remote command execution. This issue has been patched in versions 0.13.4 and 0.14.0+dev.	N/A	More Details
CVE-2026-1997	Certain HP OfficeJet Pro printers may expose information if Cross-Origin Resource Sharing (CORS) is misconfigured, potentially allowing unauthorized web origins to access device resource. CORS is disabled by default on Pro-class devices and can only be enabled by an administrator through the Embedded Web Server (EWS). Keeping CORS disabled unless explicitly required helps ensure that only trusted solutions can interact with the device.	N/A	More Details
CVE-2026-25493	Craft is a platform for creating digital experiences. In Craft versions 4.0.0-RC1 through 4.16.17 and 5.0.0-RC1 through 5.8.21, the saveAsset GraphQL mutation validates the initial URL hostname and resolved IP against a blocklist, but Guzzle follows HTTP redirects by default. An attacker can bypass all SSRF protections by hosting a redirect that points to cloud metadata endpoints or any internal IP addresses. This issue is patched in versions 4.16.18 and 5.8.22.	N/A	More Details
CVE-2026-0521	A reflected cross-site scripting (XSS) vulnerability in the PDF export functionality of the TYDAC AG MAP+ solution allows unauthenticated attackers to craft a malicious URL, that if visited by a victim, will execute arbitrary JavaScript in the victim's context. Such a URL could be delivered through various means, for instance, by sending a link or by tricking victims to visit a page crafted by the attacker. This issue was verified in MAP+: 3.4.0.	N/A	More Details
CVE-2026-25598	Harden-Runner is a CI/CD security agent that works like an EDR for GitHub Actions runners. Prior to 2.14.2, a security vulnerability has been identified in the Harden-Runner GitHub Action (Community Tier) that allows outbound network connections to evade audit logging. Specifically, outbound traffic using the sendto, sendmsg, and sendmmsg socket system calls can bypass detection and logging when using egress-policy: audit. This vulnerability is fixed in 2.14.2.	N/A	More Details
CVE-2026-25498	Craft is a platform for creating digital experiences. In versions 4.0.0-RC1 through 4.16.17 and 5.0.0-RC1 through 5.8.21, a Remote Code Execution (RCE) vulnerability exists in Craft CMS where the assembleLayoutFromPost() function in src/services/Fields.php fails to sanitize user-supplied configuration data before passing it to Craft::createObject(). This allows authenticated administrators to inject malicious Yii2 behavior configurations that execute arbitrary system commands on the server. This vulnerability represents an unpatched variant of the behavior injection vulnerability addressed in CVE-2025-68455, affecting different endpoints through a separate code path. This vulnerability is fixed in 5.8.22.	N/A	More Details
CVE-2026-25497	Craft is a platform for creating digital experiences. In Craft versions from 4.0.0-RC1 to before 4.17.0-beta.1 and 5.9.0-beta.1, there is a Privilege Escalation vulnerability in Craft CMS's GraphQL API that allows an authenticated user with write access to one asset volume to escalate their privileges and modify/transfer assets belonging to any other volume, including restricted or private volumes to which they should not have access. The saveAsset GraphQL mutation validates authorization against the schema-resolved volume but fetches the target asset by ID without verifying that the asset belongs to the authorized volume. This allows unauthorized cross-volume asset modification and transfer. This vulnerability is fixed in 4.17.0-beta.1 and 5.9.0-beta.1.	N/A	More Details
	Craft is a platform for creating digital experiences. In Craft versions 4.0.0-RC1 through		

CVE-2026-25496	Craft is a platform for creating digital experiences. In Craft versions 4.0.0-RC1 through 4.16.17 and 5.0.0-RC1 through 5.8.21, a stored XSS vulnerability exists in the Number field type settings. The Prefix and Suffix fields are rendered using the |md|raw Twig filter without proper escaping, allowing script execution when the Number field is displayed on users' profiles. This issue is patched in versions 4.16.18 and 5.8.22.	N/A	More Details
CVE-2026-25495	Craft is a platform for creating digital experiences. In Craft versions 4.0.0-RC1 through 4.16.17 and 5.0.0-RC1 through 5.8.21, the element-indexes/get-elements endpoint is vulnerable to SQL Injection via the criteria[orderBy] parameter (JSON body). The application fails to sanitize this input before using it in the database query. An attacker with Control Panel access can inject arbitrary SQL into the ORDER BY clause by omitting viewState[order] (or setting both to the same payload). This issue is patched in versions 4.16.18 and 5.8.22.	N/A	More Details
CVE-2026-25494	Craft is a platform for creating digital experiences. In Craft versions 4.0.0-RC1 through 4.16.17 and 5.0.0-RC1 through 5.8.21, the saveAsset GraphQL mutation uses filter_var(..., FILTER_VALIDATE_IP) to block a specific list of IP addresses. However, alternative IP notations (hexadecimal, mixed) are not recognized by this function, allowing attackers to bypass the blocklist and access cloud metadata services. This issue is patched in versions 4.16.18 and 5.8.22.	N/A	More Details
CVE-2026-25492	Craft CMS is a content management system. In Craft versions 3.5.0 through 4.16.17 and 5.0.0-RC1 through 5.8.21, the save_images_Asset GraphQL mutation can be abused to fetch internal URLs by providing a domain name that resolves to an internal IP address, bypassing hostname validation. When a non-image file extension such as .txt is allowed, downstream image validation is bypassed, which can allow an authenticated attacker with permission to use save_images_Asset to retrieve sensitive data such as AWS instance metadata credentials from the underlying host. This issue is patched in versions 4.16.18 and 5.8.22.	N/A	More Details
CVE-2025-7432	DPA countermeasures in Silicon Labs' Series 2 devices are not reseeded under certain conditions. This may allow an attacker to eventually extract secret keys through a DPA attack.	N/A	More Details
CVE-2026-25491	Craft is a platform for creating digital experiences. From 5.0.0-RC1 to 5.8.21, Craft has a stored XSS via Entry Type names. The name is not sanitized when displayed in the Entry Types list. This vulnerability is fixed in 5.8.22.	N/A	More Details
CVE-2025-15080	Improper Validation of Specified Quantity in Input vulnerability in Mitsubishi Electric MELSEC iQ-R Series R08PCPU, R16PCPU, R32PCPU, and R120PCPU allows an unauthenticated attacker to read device data or part of a control program from the affected product, write device data in the affected product, or cause a denial of service (DoS) condition on the affected product by sending a specially crafted packet containing a specific command to the affected product.	N/A	More Details
CVE-2026-1953	Nukegraphic CMS v3.1.2 contains a stored cross-site scripting (XSS) vulnerability in the user profile edit functionality at /ngc-cms/user-edit-profile.php. The application fails to properly sanitize user input in the name field before storing it in the database and rendering it across multiple CMS pages. An authenticated attacker with low privileges can inject malicious JavaScript payloads through the profile edit request, which are then executed site-wide whenever the affected user's name is displayed. This allows the attacker to execute arbitrary JavaScript in the context of other users' sessions, potentially leading to session hijacking, credential theft, or unauthorized actions performed on behalf of victims.	N/A	More Details
CVE-2026-25198	web2py versions 2.27.1-stable+timestamp.2023.11.16.08.03.57 and prior contain an open redirect vulnerability. If this vulnerability is exploited, the user may be redirected to an arbitrary website when accessing a specially crafted URL. As a result, the user may become a victim of a phishing attack.	N/A	More Details
CVE-2026-1966	YugabyteDB Anywhere displays LDAP bind passwords configured via gflags in cleartext within the web UI. An authenticated user with access to the configuration view could obtain LDAP credentials, potentially enabling unauthorized access to external directory services.	N/A	More Details
CVE-	Quick.Cart allows a user's session identifier to be set before authentication. The value of this session ID stays the same after authentication. This behaviour enables an attacker to fix a session ID for a victim and later hijack the authenticated session. The vendor was notified		More

2026-23796	early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only version 6.7 was tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	N/A	Details
CVE-2026-23797	In Quick.Cart user passwords are stored in plaintext form. An attacker with high privileges can display users' password in user editing page. The vendor was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Only version 6.7 was tested and confirmed as vulnerable, other versions were not tested and might also be vulnerable.	N/A	More Details
CVE-2026-25740	captive browser, a dedicated Chrome instance to log into captive portals without messing with DNS settings. In 25.05 and earlier, when programs.captive-browser is enabled, any user of the system can run arbitrary commands with the CAP_NET_RAW capability (binding to privileged ports, spoofing localhost traffic from privileged services...). This vulnerability is fixed in 25.11 and 26.05.	N/A	More Details
CVE-2025-62616	AutoGPT is a platform that allows users to create, deploy, and manage continuous artificial intelligence agents that automate complex workflows. Prior to autogpt-platform-beta-v0.6.34, in SendDiscordFileBlock, the third-party library aiohttp.ClientSession().get is used directly to access the URL, but the input URL is not filtered, which will cause SSRF vulnerability. This issue has been patched in autogpt-platform-beta-v0.6.34.	N/A	More Details
CVE-2025-62615	AutoGPT is a platform that allows users to create, deploy, and manage continuous artificial intelligence agents that automate complex workflows. Prior to autogpt-platform-beta-v0.6.34, in RSSFeedBlock, the third-party library urllib.request.urlopen is used directly to access the URL, but the input URL is not filtered, which will cause SSRF vulnerability. This issue has been patched in autogpt-platform-beta-v0.6.34.	N/A	More Details
CVE-2026-25806	PlaciPy is a placement management system designed for educational institutions. In version 1.0.0, the GET /api/students/:email PUT /api/students/:email/status, and DELETE /api/students/:email routes in backend/src/routes/student.routes.ts only enforce authentication using authenticateToken but do not enforce authorization. The application does not verify whether the authenticated user owns the student record being accessed, has an administrative / staff role, or is permitted to modify or delete the target student.	N/A	More Details
CVE-2026-21626	Access control settings for forum post custom fields are not applied to the JSON output type, leading to an ACL violation vector an information disclosure	N/A	More Details
CVE-2026-25885	PolarLearn is a free and open-source learning program. In 0-PRERELEASE-16 and earlier, the group chat WebSocket at wss://polarlearn.nl/api/v1/ws can be used without logging in. An unauthenticated client can subscribe to any group chat by providing a group UUID, and can also send messages to any group. The server accepts the message and stores it in the group’s chatContent, so this is not just a visual spam issue.	N/A	More Details
CVE-2026-25543	HtmlSanitizer is a .NET library for cleaning HTML fragments and documents from constructs that can lead to XSS attacks. Prior to versions 9.0.892 and 9.1.893-beta, if the template tag is allowed, its contents are not sanitized. The template tag is a special tag that does not usually render its contents, unless the shadowrootmode attribute is set to open or closed. This issue has been patched in versions 9.0.892 and 9.1.893-beta.	N/A	More Details
CVE-2026-25875	PlaciPy is a placement management system designed for educational institutions. In version 1.0.0, The admin authorization middleware trusts client-controlled JWT claims (role and scope) without enforcing server-side role verification.	N/A	More Details
CVE-2026-25814	PlaciPy is a placement management system designed for educational institutions. In version 1.0.0, User-controlled query parameters are passed directly into DynamoDB query/filter construction without validation or sanitization.	N/A	More Details
CVE-2026-25813	PlaciPy is a placement management system designed for educational institutions. In version 1.0.0, The application logs highly sensitive data directly to console output without masking or redaction.	N/A	More Details
CVE-	PlaciPy is a placement management system designed for educational institutions. In version		

2026-25812	1.0.0, the application enables credentialed CORS requests but does not implement any CSRF protection mechanism.	N/A	More Details
CVE-2026-25811	PlaciPy is a placement management system designed for educational institutions. In version 1.0.0, the application derives the tenant identifier directly from the email domain provided by the user, without validating domain ownership or registration. This allows cross-tenant data access.	N/A	More Details
CVE-2026-25547	@isaacs/brace-expansion is a hybrid CJS/ESM TypeScript fork of brace-expansion. Prior to version 5.0.1, @isaacs/brace-expansion is vulnerable to a denial of service (DoS) issue caused by unbounded brace range expansion. When an attacker provides a pattern containing repeated numeric brace ranges, the library attempts to eagerly generate every possible combination synchronously. Because the expansion grows exponentially, even a small input can consume excessive CPU and memory and may crash the Node.js process. This issue has been patched in version 5.0.1.	N/A	More Details
CVE-2026-25575	NavigaTUM is a website and API to search for rooms, buildings and other places. Prior to commit 86f34c7, there is a path traversal vulnerability in the propose_edits endpoint allows unauthenticated users to overwrite files in directories writable by the application user (e.g., /cdn). By supplying unsanitized file keys containing traversal sequences (e.g., ../../) in the JSON payload, an attacker can escape the intended temporary directory and replace public facing images or fill the server's storage. This issue has been patched via commit 86f34c7.	N/A	More Details
CVE-2026-25579	Navidrome is an open source web-based music collection server and streamer. Prior to version 0.60.0, authenticated users can crash the Navidrome server by supplying an excessively large size parameter to /rest/getCoverArt or to a shared-image URL (/share/img/<token>). When processing such requests, the server attempts to create an extremely large resized image, causing uncontrolled memory growth. This triggers the Linux OOM killer, terminates the Navidrome process, and results in a full service outage. If the system has sufficient memory and survives the allocation, Navidrome then writes these extremely large resized images into its cache directory, allowing an attacker to rapidly exhaust server disk space as well. This issue has been patched in version 0.60.0.	N/A	More Details
CVE-2026-25878	FroshAdminer is the Adminer plugin for Shopware Platform. Prior to 2.2.1, the Adminer route (/admin/adminer) was accessible without Shopware admin authentication. The route was configured with auth_required=false and performed no session validation, exposing the Adminer UI to unauthenticated users. This vulnerability is fixed in 2.2.1.	N/A	More Details
CVE-2026-25876	PlaciPy is a placement management system designed for educational institutions. In version 1.0.0, the backend/src/routes/results.routes.ts verify authentication but fails to enforce object-level authorization (ownership checks). For example, this can be used to return all results for an assessment.	N/A	More Details
CVE-2026-25810	PlaciPy is a placement management system designed for educational institutions. In version 1.0.0, the backend/src/routes/student.submission.routes.ts verify authentication but fails to enforce object-level authorization (ownership checks).	N/A	More Details
CVE-2026-25809	PlaciPy is a placement management system designed for educational institutions. In version 1.0.0, the code evaluation endpoint does not validate the assessment lifecycle state before allowing execution. There is no check to ensure that the assessment has started, is not expired, or the submission window is currently open.	N/A	More Details
CVE-2026-1523	Path Traversal vulnerability in Digitek ADT1100 and Digitek DT950 from PRIMION DIGITEK, S.L.U (Azkoyen Group). This vulnerability allows an attacker to access arbitrary files in the server's file system, thet is, 'http://<host>/..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd'. By manipulating the input to include URL encoded directory traversal sequences (e.g., %2F representing /), an attacker can bypass the input validation mechanisms ans retrieve sensitive files outside the intended directory, which could lead to information disclosure or further system compromise.	N/A	More Details
CVE-	Fiber is an Express inspired web framework written in Go. Before 2.52.11, on Go versions prior to 1.24, the underlying crypto/rand implementation can return an error if secure randomness cannot be obtained. Because no error is returned by the Fiber v2 UUID		More

2025-66630	functions, application code may unknowingly rely on predictable, repeated, or low-entropy identifiers in security-critical pathways. This is especially impactful because many Fiber v2 middleware components (session middleware, CSRF, rate limiting, request-ID generation, etc.) default to using utils.UUIDv4(). This vulnerability is fixed in 2.52.11.	N/A	More Details
CVE-2026-1996	Certain HP OfficeJet Pro printers may be vulnerable to potential denial of service when the IPP requests are mishandled, failing to establish a TCP connection.	N/A	More Details
CVE-2025-66603	A vulnerability has been found in FAST/TOOLS provided by Yokogawa Electric Corporation. The web server accepts the OPTIONS method. An attacker could potentially use this information to carry out other attacks. The affected products and versions are as follows: FAST/TOOLS (Packages: RVSVRN, UNSVRN, HMIWEB, FTEES, HMIMOB) R9.01 to R10.04	N/A	More Details
CVE-2025-47911	The html.Parse function in golang.org/x/net/html has quadratic parsing complexity when processing certain inputs, which can lead to denial of service (DoS) if an attacker provides specially crafted HTML content.	N/A	More Details
CVE-2025-58190	The html.Parse function in golang.org/x/net/html has an infinite parsing loop when processing certain inputs, which can lead to denial of service (DoS) if an attacker provides specially crafted HTML content.	N/A	More Details
CVE-2025-66608	A vulnerability has been found in FAST/TOOLS provided by Yokogawa Electric Corporation. This product does not properly validate URLs. An attacker could send specially crafted requests to steal files from the web server. The affected products and versions are as follows: FAST/TOOLS (Packages: RVSVRN, UNSVRN, HMIWEB, FTEES, HMIMOB) R9.01 to R10.04	N/A	More Details
CVE-2025-66607	A vulnerability has been found in FAST/TOOLS provided by Yokogawa Electric Corporation. The response header contains an insecure setting. Users could be redirected to malicious sites by an attacker. The affected products and versions are as follows: FAST/TOOLS (Packages: RVSVRN, UNSVRN, HMIWEB, FTEES, HMIMOB) R9.01 to R10.04	N/A	More Details
CVE-2025-66606	A vulnerability has been found in FAST/TOOLS provided by Yokogawa Electric Corporation. This product does not properly encode URLs. An attacker could tamper with web pages or execute malicious scripts. The affected products and versions are as follows: FAST/TOOLS (Packages: RVSVRN, UNSVRN, HMIWEB, FTEES, HMIMOB) R9.01 to R10.04	N/A	More Details
CVE-2025-66605	A vulnerability has been found in FAST/TOOLS provided by Yokogawa Electric Corporation. Since there are input fields on this webpage with the autocomplete attribute enabled, the input content could be saved in the browser the user is using. The affected products and versions are as follows: FAST/TOOLS (Packages: RVSVRN, UNSVRN, HMIWEB, FTEES, HMIMOB) R9.01 to R10.04	N/A	More Details
CVE-2025-66604	A vulnerability has been found in FAST/TOOLS provided by Yokogawa Electric Corporation. The library version could be displayed on the web page. This information could be exploited by an attacker for other attacks. The affected products and versions are as follows: FAST/TOOLS (Packages: RVSVRN, UNSVRN, HMIWEB, FTEES, HMIMOB) R9.01 to R10.04	N/A	More Details
CVE-2025-66602	A vulnerability has been found in FAST/TOOLS provided by Yokogawa Electric Corporation. The web server accepts access by IP address. When a worm that randomly searches for IP addresses intrudes into the network, it could potentially be attacked by the worm. The affected products and versions are as follows: FAST/TOOLS (Packages: RVSVRN, UNSVRN, HMIWEB, FTEES, HMIMOB) R9.01 to R10.04	N/A	More Details
CVE-2026-24095	Improper permission enforcement in Checkmk versions 2.4.0 before 2.4.0p21, 2.3.0 before 2.3.0p43, and 2.2.0 (EOL) allows users with the "Use WATO" permission to access the "Analyze configuration" page by directly navigating to its URL, bypassing the intended "Access analyze configuration" permission check. If these users also have the "Make changes, perform actions" permission, they can perform unauthorized actions such as disabling checks or acknowledging results.	N/A	More Details
CVE-	A vulnerability has been found in FAST/TOOLS provided by Yokogawa Electric Corporation. This product does not specify MIME types. When an attacker performs a content sniffing		More

2025-66601	attack, malicious scripts could be executed. The affected products and versions are as follows: FAST/TOOLS (Packages: RVSVRN, UNSVRN, HMIWEB, FTEES, HMIMOB) R9.01 to R10.04	N/A	More Details
CVE-2025-66600	A vulnerability has been found in FAST/TOOLS provided by Yokogawa Electric Corporation. This product lacks HSTS (HTTP Strict Transport Security) configuration. When an attacker performs a Man in the middle (MITM) attack, communications with the web server could be sniffed. The affected products and versions are as follows: FAST/TOOLS (Packages: RVSVRN, UNSVRN, HMIWEB, FTEES, HMIMOB) R9.01 to R10.04	N/A	More Details
CVE-2025-66599	A vulnerability has been found in FAST/TOOLS provided by Yokogawa Electric Corporation. Physical paths could be displayed on web pages. This information could be exploited by an attacker for other attacks. The affected products and versions are as follows: FAST/TOOLS (Packages: RVSVRN, UNSVRN, HMIWEB, FTEES, HMIMOB) R9.01 to R10.04	N/A	More Details
CVE-2026-1301	In builds with PubSub and JSON enabled, a crafted JSON message can cause the decoder to write beyond a heap-allocated array before authentication, reliably crashing the process and corrupting memory.	N/A	More Details
CVE-2026-25630	Rejected reason: Reason: This candidate was issued in error.	N/A	More Details
CVE-2025-12131	A truncated 802.15.4 packet can lead to an assert, resulting in a denial of service.	N/A	More Details
CVE-2025-32393	AutoGPT is a platform that allows users to create, deploy, and manage continuous artificial intelligence agents that automate complex workflows. Prior to autogpt-platform-beta-v0.6.32, there is a DoS vulnerability in ReadRSSFeedBlock. In RSSBlock, feedparser.parser is called to obtain the XML file according to the URL input by the user, parse the XML, and finally obtain the parsed result. However, during the parsing process, there is no limit on the parsing time and the resources that can be allocated for parsing. When a malicious user lets RSSBlock parse a carefully constructed, deep XML, it will cause memory resources to be exhausted, eventually causing DoS. This issue has been patched in autogpt-platform-beta-v0.6.32.	N/A	More Details
CVE-2025-66594	A vulnerability has been found in FAST/TOOLS provided by Yokogawa Electric Corporation. Detailed messages are displayed on the error page. This information could be exploited by an attacker for other attacks. The affected products and versions are as follows: FAST/TOOLS (Packages: RVSVRN, UNSVRN, HMIWEB, FTEES, HMIMOB) R9.01 to R10.04	N/A	More Details
CVE-2025-66595	A vulnerability has been found in FAST/TOOLS provided by Yokogawa Electric Corporation. This product is vulnerable to Cross-Site Request Forgery (CSRF). When a user accesses a link crafted by an attacker, the user’s account could be compromised. The affected products and versions are as follows: FAST/TOOLS (Packages: RVSVRN, UNSVRN, HMIWEB, FTEES, HMIMOB) R9.01 to R10.04	N/A	More Details
CVE-2025-66596	A vulnerability has been found in FAST/TOOLS provided by Yokogawa Electric Corporation. This product does not properly validate request headers. When an attacker inserts an invalid host header, users could be redirected to malicious sites. The affected products and versions are as follows: FAST/TOOLS (Packages: RVSVRN, UNSVRN, HMIWEB, FTEES, HMIMOB) R9.01 to R10.04	N/A	More Details
CVE-2025-66597	A vulnerability has been found in FAST/TOOLS provided by Yokogawa Electric Corporation. This product supports weak cryptographic algorithms, potentially allowing an attacker to decrypt communications with the web server. The affected products and versions are as follows: FAST/TOOLS (Packages: RVSVRN, UNSVRN, HMIWEB, FTEES, HMIMOB) R9.01 to R10.04	N/A	More Details
CVE-2026-25698	Rejected reason: Not used	N/A	More Details

CVE-2026-1960	Stored Cross-Site Scripting (XSS) vulnerability in Loggro Pymes, via the 'Facebook' parameter in '/loggrodemo/jbrain/ConsultaTerceros' endpoint.	N/A	More Details
CVE-2026-1959	Stored Cross-Site Scripting (XSS) vulnerability in Loggro Pymes, via the 'descripción' parameter in the '/loggrodemo/jbrain/MaestraCuentasBancarias' endpoint.	N/A	More Details
CVE-2026-25697	Rejected reason: Not used	N/A	More Details
CVE-2026-25696	Rejected reason: Not used	N/A	More Details
CVE-2026-25695	Rejected reason: Not used	N/A	More Details
CVE-2026-25694	Rejected reason: Not used	N/A	More Details
CVE-2026-25693	Rejected reason: Not used	N/A	More Details
CVE-2026-25692	Rejected reason: Not used	N/A	More Details
CVE-2026-0714	A physical attack vulnerability exists in certain Moxa industrial computers using TPM-backed LUKS full-disk encryption on Moxa Industrial Linux 3, where the discrete TPM is connected to the CPU via an SPI bus. Exploitation requires invasive physical access, including opening the device and attaching external equipment to the SPI bus to capture TPM communications. If successful, the captured data may allow offline decryption of eMMC contents. This attack cannot be performed through brief or opportunistic physical access and requires extended physical access, possession of the device, appropriate equipment, and sufficient time for signal capture and analysis. Remote exploitation is not possible.	N/A	More Details
CVE-2026-24466	Products provided by Oki Electric Industry Co., Ltd. and its OEM products (Ricoh Co., Ltd., Murata Machinery, Ltd.) register Windows services with unquoted file paths. A user with the write permission on the root directory of the system drive may execute arbitrary code with SYSTEM privilege.	N/A	More Details
CVE-2026-0715	Moxa Arm-based industrial computers running Moxa Industrial Linux Secure use a device-unique bootloader password provided on the device. An attacker with physical access to the device could use this information to access the bootloader menu via a serial interface. Access to the bootloader menu does not allow full system takeover or privilege escalation. The bootloader enforces digital signature verification and only permits flashing of Moxa-signed images. As a result, an attacker cannot install malicious firmware or execute arbitrary code. The primary impact is limited to a potential temporary denial-of-service condition if a valid image is reflashed. Remote exploitation is not possible.	N/A	More Details
CVE-2025-15551	The response coming from TP-Link Archer MR200 v5.2, C20 v6, TL-WR850N v3, and TL-WR845N v4 for any request is getting executed by the JavaScript function like eval directly without any check. Attackers can exploit this vulnerability via a Man-in-the-Middle (MitM) attack to execute JavaScript code on the router's admin web portal without the user's permission or knowledge.	N/A	More Details
CVE-2025-15557	An Improper Certificate Validation vulnerability in TP-Link Tapo H100 v1 and Tapo P100 v1 allows an on-path attacker on the same network segment to intercept and modify encrypted device-cloud communications. This may compromise the confidentiality and integrity of	N/A	More Details

	device-to-cloud communication, enabling manipulation of device data or operations.		
CVE-2025-66598	A vulnerability has been found in FAST/TOOLS provided by Yokogawa Electric Corporation. This product supports old SSL/TLS versions, potentially allowing an attacker to decrypt communications with the web server. The affected products and versions are as follows: FAST/TOOLS (Packages: RVSVRN, UNSVRN, HMIWEB, FTEES, HMIMOB) R9.01 to R10.04	N/A	More Details
CVE-2026-25541	Bytes is a utility library for working with bytes. From version 1.2.1 to before 1.11.1, Bytes is vulnerable to integer overflow in BytesMut::reserve. In the unique reclaim path of BytesMut::reserve, if the condition "v_capacity >= new_cap + offset" uses an unchecked addition. When new_cap + offset overflows usize in release builds, this condition may incorrectly pass, causing self.cap to be set to a value that exceeds the actual allocated capacity. Subsequent APIs such as spare_capacity_mut() then trust this corrupted cap value and may create out-of-bounds slices, leading to UB. This behavior is observable in release builds (integer overflow wraps), whereas debug builds panic due to overflow checks. This issue has been patched in version 1.11.1.	N/A	More Details
CVE-2026-25538	Devtron is an open source tool integration platform for Kubernetes. In version 2.0.0 and prior, a vulnerability exists in Devtron's Attributes API interface, allowing any authenticated user (including low-privileged CI/CD Developers) to obtain the global API Token signing key by accessing the /orchestrator/attributes?key=apiTokenSecret endpoint. After obtaining the key, attackers can forge JWT tokens for arbitrary user identities offline, thereby gaining complete control over the Devtron platform and laterally moving to the underlying Kubernetes cluster. This issue has been patched via commit d2b0d26.	N/A	More Details
CVE-2026-25918	unity-cli is a command line utility for the Unity Game Engine. Prior to 1.8.2 , the sign-package command in @rage-against-the-pixel/unity-cli logs sensitive credentials in plaintext when the --verbose flag is used. Command-line arguments including --email and --password are output via JSON.stringify without sanitization, exposing secrets to shell history, CI/CD logs, and log aggregation systems. This vulnerability is fixed in 1.8.2.	N/A	More Details
CVE-2026-23105	In the Linux kernel, the following vulnerability has been resolved: net/sched: qfq: Use cl_is_active to determine whether class is active in qfq_rm_from_ag This is more of a preventive patch to make the code more consistent and to prevent possible exploits that employ child qlen manipulations on qfq. use cl_is_active instead of relying on the child qdisc's qlen to determine class activation.	N/A	More Details
CVE-2026-24851	OpenFGA is a high-performance and flexible authorization/permission engine built for developers and inspired by Google Zanzibar. OpenFGA v1.8.5 to v1.11.2 (openfga-0.2.22<= Helm chart <= openfga-0.2.51, v.1.8.5 <= docker <= v.1.11.2) are vulnerable to improper policy enforcement when certain Check calls are executed. The vulnerability requires a model that has a a relation directly assignable by a type bound public access and assignable by type bound non-public access, a tuple assigned for the relation that is a type bound public access, a tuple assigned for the same object with the same relation that is not type bound public access, and a tuple assigned for a different object that has an object ID lexicographically larger with the same user and relation which is not type bound public access. This vulnerability is fixed in v1.11.3.	N/A	More Details
CVE-	In the Linux kernel, the following vulnerability has been resolved: bonding: limit BOND_MODE_8023AD to Ethernet devices BOND_MODE_8023AD makes sense for ARPHRD_ETHER only. syzbot reported: BUG: KASAN: global-out-of-bounds in __hw_addr_create net/core/dev_addr_lists.c:63 [inline] BUG: KASAN: global-out-of-bounds in __hw_addr_add_ex+0x25d/0x760 net/core/dev_addr_lists.c:118 Read of size 16 at addr ffffffff8bf94040 by task syz.1.3580/19497 CPU: 1 UID: 0 PID: 19497 Comm: syz.1.3580 Tainted: G L syzkaller #0 PREEMPT(full) Tainted: [L]=SOFTLOCKUP Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 10/25/2025 Call Trace: <TASK> dump_stack_lvl+0xe8/0x150 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:378 [inline] print_report+0xca/0x240 mm/kasan/report.c:482 kasan_report+0x118/0x150 mm/kasan/report.c:595 check_region_inline mm/kasan/generic.c:-1 [inline] kasan_check_range+0x2b0/0x2c0 mm/kasan/generic.c:200 __asan_memcpy+0x29/0x70 mm/kasan/shadow.c:105 __hw_addr_create net/core/dev_addr_lists.c:63 [inline] __hw_addr_add_ex+0x25d/0x760 net/core/dev_addr_lists.c:118 __dev_mc_add net/core/dev_addr_lists.c:868 [inline]		

2026-23099	dev_mc_add+0xa1/0x120 net/core/dev_addr_lists.c:886 bond_enslave+0x2b8b/0x3ac0 drivers/net/bonding/bond_main.c:2180 do_set_master+0x533/0x6d0 net/core/rtnetlink.c:2963 do_setlink+0xcf0/0x41c0 net/core/rtnetlink.c:3165 rtnl_changelink net/core/rtnetlink.c:3776 [inline] __rtnl_newlink net/core/rtnetlink.c:3935 [inline] rtnl_newlink+0x161c/0x1c90 net/core/rtnetlink.c:4072 rtnetlink_rcv_msg+0x7cf/0xb70 net/core/rtnetlink.c:6958 netlink_rcv_skb+0x208/0x470 net/netlink/af_netlink.c:2550 netlink_unicast_kernel net/netlink/af_netlink.c:1318 [inline] netlink_unicast+0x82f/0x9e0 net/netlink/af_netlink.c:1344 netlink_sendmsg+0x805/0xb30 net/netlink/af_netlink.c:1894 sock_sendmsg_nosec net/socket.c:727 [inline] __sock_sendmsg+0x21c/0x270 net/socket.c:742 ____sys_sendmsg+0x505/0x820 net/socket.c:2592 ___sys_sendmsg+0x21f/0x2a0 net/socket.c:2646 __sys_sendmsg+0x164/0x220 net/socket.c:2678 do_syscall_32_irqs_on arch/x86/entry/syscall_32.c:83 [inline] __do_fast_syscall_32+0x1dc/0x560 arch/x86/entry/syscall_32.c:307 do_fast_syscall_32+0x34/0x80 arch/x86/entry/syscall_32.c:332 entry_SYSENTER_compat_after_hwframe+0x84/0x8e </TASK> The buggy address belongs to the variable: lacpdu_mcast_addr+0x0/0x40	N/A	More Details
CVE-2026-23100	In the Linux kernel, the following vulnerability has been resolved: mm/hugetlb: fix hugetlb_pmd_shared() Patch series "mm/hugetlb: fixes for PMD table sharing (incl. using mmu_gather)", v3. One functional fix, one performance regression fix, and two related comment fixes. I cleaned up my prototype I recently shared [1] for the performance fix, deferring most of the cleanups I had in the prototype to a later point. While doing that I identified the other things. The goal of this patch set is to be backported to stable trees "fairly" easily. At least patch #1 and #4. Patch #1 fixes hugetlb_pmd_shared() not detecting any sharing Patch #2 + #3 are simple comment fixes that patch #4 interacts with. Patch #4 is a fix for the reported performance regression due to excessive IPI broadcasts during fork()+exit(). The last patch is all about TLB flushes, IPIs and mmu_gather. Read: complicated There are plenty of cleanups in the future to be had + one reasonable optimization on x86. But that's all out of scope for this series. Runtime tested, with a focus on fixing the performance regression using the original reproducer [2] on x86. This patch (of 4): We switched from (wrongly) using the page count to an independent shared count. Now, shared page tables have a refcount of 1 (excluding speculative references) and instead use ptdesc->pt_share_count to identify sharing. We didn't convert hugetlb_pmd_shared(), so right now, we would never detect a shared PMD table as such, because sharing/unsharing no longer touches the refcount of a PMD table. Page migration, like mbind() or migrate_pages() would allow for migrating folios mapped into such shared PMD tables, even though the folios are not exclusive. In smaps we would account them as "private" although they are "shared", and we would be wrongly setting the PM_MMAP_EXCLUSIVE in the pagemap interface. Fix it by properly using ptdesc_pmd_is_shared() in hugetlb_pmd_shared().	N/A	More Details
CVE-2026-23101	In the Linux kernel, the following vulnerability has been resolved: leds: led-class: Only Add LED to leds_list when it is fully ready Before this change the LED was added to leds_list before led_init_core() gets called adding it the list before led_classdev.set_brightness_work gets initialized. This leaves a window where led_trigger_register() of a LED's default trigger will call led_trigger_set() which calls led_set_brightness() which in turn will end up queueing the *uninitialized* led_classdev.set_brightness_work. This race gets hit by the lenovo-thinkpad-t14s EC driver which registers 2 LEDs with a default trigger provided by snd_ctl_led.ko in quick succession. The first led_classdev_register() causes an async modprobe of snd_ctl_led to run and that async modprobe manages to exactly hit the window where the second LED is on the leds_list without led_init_core() being called for it, resulting in: ------------[cut here]------------ WARNING: CPU: 11 PID: 5608 at kernel/workqueue.c:4234 __flush_work+0x344/0x390 Hardware name: LENOVO 21N2S01F0B/21N2S01F0B, BIOS N42ET93W (2.23) 09/01/2025 ... Call trace: __flush_work+0x344/0x390 (P) flush_work+0x2c/0x50 led_trigger_set+0x1c8/0x340 led_trigger_register+0x17c/0x1c0 led_trigger_register_simple+0x84/0xe8 snd_ctl_led_init+0x40/0xf88 [snd_ctl_led] do_one_initcall+0x5c/0x318 do_init_module+0x9c/0x2b8 load_module+0x7e0/0x998 Close the race window by moving the adding of the LED to leds_list to after the led_init_core() call.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: arm64/fpsimd: signal: Fix		

CVE-2026-23102	In the Linux kernel, the following vulnerability has been resolved: arm64/fpsimd: signal: Fix restoration of SVE context When SME is supported, Restoring SVE signal context can go wrong in a few ways, including placing the task into an invalid state where the kernel may read from out-of-bounds memory (and may potentially take a fatal fault) and/or may kill the task with a SIGKILL. (1) Restoring a context with SVE_SIG_FLAG_SM set can place the task into an invalid state where SVCR.SM is set (and sve_state is non-NULL) but TIF_SME is clear, consequently resuting in out-of-bounds memory reads and/or killing the task with SIGKILL. This can only occur in unusual (but legitimate) cases where the SVE signal context has either been modified by userspace or was saved in the context of another task (e.g. as with CRIU), as otherwise the presence of an SVE signal context with SVE_SIG_FLAG_SM implies that TIF_SME is already set. While in this state, task_fpsimd_load() will NOT configure SMCR_ELx (leaving some arbitrary value configured in hardware) before restoring SVCR and attempting to restore the streaming mode SVE registers from memory via sve_load_state(). As the value of SMCR_ELx.LEN may be larger than the task's streaming SVE vector length, this may read memory outside of the task's allocated sve_state, reading unrelated data and/or triggering a fault. While this can result in secrets being loaded into streaming SVE registers, these values are never exposed. As TIF_SME is clear, fpsimd_bind_task_to_cpu() will configure CPACR_ELx.SMEN to trap EL0 accesses to streaming mode SVE registers, so these cannot be accessed directly at EL0. As fpsimd_save_user_state() verifies the live vector length before saving (S)SVE state to memory, no secret values can be saved back to memory (and hence cannot be observed via ptrace, signals, etc). When the live vector length doesn't match the expected vector length for the task, fpsimd_save_user_state() will send a fatal SIGKILL signal to the task. Hence the task may be killed after executing userspace for some period of time. (2) Restoring a context with SVE_SIG_FLAG_SM clear does not clear the task's SVCR.SM. If SVCR.SM was set prior to restoring the context, then the task will be left in streaming mode unexpectedly, and some register state will be combined inconsistently, though the task will be left in legitimate state from the kernel's PoV. This can only occur in unusual (but legitimate) cases where ptrace has been used to set SVCR.SM after entry to the sigreturn syscall, as syscall entry clears SVCR.SM. In these cases, the the provided SVE register data will be loaded into the task's sve_state using the non-streaming SVE vector length and the FPSIMD registers will be merged into this using the streaming SVE vector length. Fix (1) by setting TIF_SME when setting SVCR.SM. This also requires ensuring that the task's sme_state has been allocated, but as this could contain live ZA state, it should not be zeroed. Fix (2) by clearing SVCR.SM when restoring a SVE signal context with SVE_SIG_FLAG_SM clear. For consistency, I've pulled the manipulation of SVCR, TIF_SVE, TIF_SME, and fp_type earlier, immediately after the allocation of sve_state/sme_state, before the restore of the actual register state. This makes it easier to ensure that these are always modified consistently, even if a fault is taken while reading the register data from the signal context. I do not expect any software to depend on the exact state restored when a fault is taken while reading the context.	N/A	More Details
CVE-2026-23103	In the Linux kernel, the following vulnerability has been resolved: ipvlan: Make the addrs_lock be per port Make the addrs_lock be per port, not per ipvlan dev. Initial code seems to be written in the assumption, that any address change must occur under RTNL. But it is not so for the case of IPv6. So 1) Introduce per-port addrs_lock. 2) It was needed to fix places where it was forgotten to take lock (ipvlan_open/ipvlan_close) This appears to be a very minor problem though. Since it's highly unlikely that ipvlan_add_addr() will be called on 2 CPU simultaneously. But nevertheless, this could cause: 1) False-negative of ipvlan_addr_busy(): one interface iterated through all port->ipvlans + ipvlan->addrs under some ipvlan spinlock, and another added IP under its own lock. Though this is only possible for IPv6, since looks like only ipvlan_addr6_event() can be called without rtnl_lock. 2) Race since ipvlan_ht_addr_add(port) is called under different ipvlan->addrs_lock locks This should not affect performance, since add/remove IP is a rare situation and spinlock is not taken on fast paths.	N/A	More Details
CVE-2026-	In the Linux kernel, the following vulnerability has been resolved: ice: fix devlink reload call trace Commit 4da71a77fc3b ("ice: read internal temperature sensor") introduced internal temperature sensor reading via HWMON. ice_hwmon_init() was added to ice_init_feature() and ice_hwmon_exit() was added to ice_remove(). As a result if devlink reload is used to reinit the device and then the driver is removed, a call trace can occur. BUG: unable to handle page fault for address: ffffffffc0fd4b5d Call Trace: string+0x48/0xe0 vsnprintf+0x1f9/0x650 sprintf+0x62/0x80 name_show+0x1f/0x30 dev_attr_show+0x19/0x60 The call trace repeats approximately every 10 minutes when	N/A	More

2026-23104	system monitoring tools (e.g., sadc) attempt to read the orphaned hwmon sysfs attributes that reference freed module memory. The sequence is: 1. Driver load, ice_hwmon_init() gets called from ice_init_feature() 2. Devlink reload down, flow does not call ice_remove() 3. Devlink reload up, ice_hwmon_init() gets called from ice_init_feature() resulting in a second instance 4. Driver unload, ice_hwmon_exit() called from ice_remove() leaving the first hwmon instance orphaned with dangling pointer Fix this by moving ice_hwmon_exit() from ice_remove() to ice_deinit_features() to ensure proper cleanup symmetry with ice_hwmon_init().	N/A	Details
CVE-2026-1774	CASL Ability, versions 2.4.0 through 6.7.4, contains a prototype pollution vulnerability.	N/A	More Details
CVE-2026-25923	my little forum is a PHP and MySQL based internet forum that displays the messages in classical threaded view. Prior to 20260208.1, the application fails to filter the phar:// protocol in URL validation, allowing attackers to upload a malicious Phar Polyglot file (disguised as JPEG) via the image upload feature, trigger Phar deserialization through BBCode [img] tag processing, and exploit Smarty 4.1.0 POP chain to achieve arbitrary file deletion. This vulnerability is fixed in 20260208.1.	N/A	More Details
CVE-2026-23106	In the Linux kernel, the following vulnerability has been resolved: timekeeping: Adjust the leap state for the correct auxiliary timekeeper When __do_ajdtimex() was introduced to handle adjtimex for any timekeeper, this reference to tk_core was not updated. When called on an auxiliary timekeeper, the core timekeeper would be updated incorrectly. This gets caught by the lock debugging diagnostics because the timekeepers sequence lock gets written to without holding its associated spinlock: WARNING: include/linux/seqlock.h:226 at __do_adjtimex+0x394/0x3b0, CPU#2: test/125 aux_clock_adj (kernel/time/timekeeping.c:2979) __do_sys_clock_adjtime (kernel/time/posix-timers.c:1161 kernel/time/posix-timers.c:1173) do_syscall_64 (arch/x86/entry/syscall_64.c:63 (discriminator 1) arch/x86/entry/syscall_64.c:94 (discriminator 1)) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:131) Update the correct auxiliary timekeeper.	N/A	More Details
CVE-2026-23107	In the Linux kernel, the following vulnerability has been resolved: arm64/fpsimd: signal: Allocate SSVE storage when restoring ZA The code to restore a ZA context doesn't attempt to allocate the task's sve_state before setting TIF_SME. Consequently, restoring a ZA context can place a task into an invalid state where TIF_SME is set but the task's sve_state is NULL. In legitimate but uncommon cases where the ZA signal context was NOT created by the kernel in the context of the same task (e.g. if the task is saved/restored with something like CRIU), we have no guarantee that sve_state had been allocated previously. In these cases, userspace can enter streaming mode without trapping while sve_state is NULL, causing a later NULL pointer dereference when the kernel attempts to store the register state: | # ./sigreturn-za | Unable to handle kernel NULL pointer dereference at virtual address 0000000000000000 | Mem abort info: | ESR = 0x0000000096000046 | EC = 0x25: DABT (current EL), IL = 32 bits | SET = 0, FnV = 0 | EA = 0, S1PTW = 0 | FSC = 0x06: level 2 translation fault | Data abort info: | ISV = 0, ISS = 0x00000046, ISS2 = 0x00000000 | CM = 0, WnR = 1, TnD = 0, TagAccess = 0 | GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 | user pgtable: 4k pages, 52-bit VAs, pgdp=0000000101f47c00 | [0000000000000000] pgd=08000001021d8403, p4d=0800000102274403, pud=0800000102275403, pmd=0000000000000000 | Internal error: Oops: 0000000096000046 [#1] SMP | Modules linked in: | CPU: 0 UID: 0 PID: 153 Comm: sigreturn-za Not tainted 6.19.0-rc1 #1 PREEMPT | Hardware name: linux,dummy-virt (DT) | pstate: 214000c9 (nzCv daIF +PAN -UAO -TCO +DIT -SSBS BTYPE=--) | pc : sve_save_state+0x4/0xf0 | lr : fpsimd_save_user_state+0xb0/0x1c0 | sp : ffff80008070bcc0 | x29: ffff80008070bcc0 x28: fff00000c1ca4c40 x27: 63cfa172fb5cf658 | x26: fff00000c1ca5228 x25: 0000000000000000 x24: 0000000000000000 | x23: 0000000000000000 x22: fff00000c1ca4c40 x21: fff00000c1ca4c40 | x20: 0000000000000020 x19: fff00000ff6900f0 x18: 0000000000000000 | x17: fff05e8e0311f000 x16: 0000000000000000 x15: 028fca8f3bdaf21c | x14: 0000000000000212 x13: fff00000c0209f10 x12: 0000000000000020 | x11: 0000000000200b20 x10: 0000000000000000 x9 : fff00000ff69dcc0 | x8 : 00000000000003f2 x7 : 0000000000000001 x6 : fff00000c1ca5b48 | x5 : fff05e8e0311f000 x4 : 0000000008000000 x3 : 0000000000000000 | x2 :	N/A	More Details

	0000000000000001 x1 : fff00000c1ca5970 x0 : 0000000000000440 | Call trace: | sve_save_state+0x4/0xf0 (P) | fpsimd_thread_switch+0x48/0x198 | __switch_to+0x20/0x1c0 | __schedule+0x36c/0xce0 | schedule+0x34/0x11c | exit_to_user_mode_loop+0x124/0x188 | el0_interrupt+0xc8/0xd8 | __el0_irq_handler_common+0x18/0x24 | el0t_64_irq_handler+0x10/0x1c | el0t_64_irq+0x198/0x19c | Code: 54000040 d51b4408 d65f03c0 d503245f (e5bb5800) | ---[end trace 0000000000000000]--- Fix this by having restore_za_context() ensure that the task's sve_state is allocated, matching what we do when taking an SME trap. Any live SVE/SSVE state (which is restored earlier from a separate signal context) must be preserved, and hence this is not zeroed.		
CVE-2026-23108	In the Linux kernel, the following vulnerability has been resolved: can: usb_8dev: usb_8dev_read_bulk_callback(): fix URB memory leak Fix similar memory leak as in commit 7352e1d5932a ("can: gs_usb: gs_usb_receive_bulk_callback(): fix URB memory leak"). In usb_8dev_open() -> usb_8dev_start(), the URBs for USB-in transfers are allocated, added to the priv->rx_submitted anchor and submitted. In the complete callback usb_8dev_read_bulk_callback(), the URBs are processed and resubmitted. In usb_8dev_close() -> unlink_all_urbs() the URBs are freed by calling usb_kill_anchored_urbs(&priv->rx_submitted). However, this does not take into account that the USB framework unanchors the URB before the complete function is called. This means that once an in-URB has been completed, it is no longer anchored and is ultimately not released in usb_kill_anchored_urbs(). Fix the memory leak by anchoring the URB in the usb_8dev_read_bulk_callback() to the priv->rx_submitted anchor.	N/A	More Details
CVE-2026-23109	In the Linux kernel, the following vulnerability has been resolved: fs/writeback: skip AS_NO_DATA_INTEGRITY mappings in wait_sb_inodes() Above the while() loop in wait_sb_inodes(), we document that we must wait for all pages under writeback for data integrity. Consequently, if a mapping, like fuse, traditionally does not have data integrity semantics, there is no need to wait at all; we can simply skip these inodes. This restores fuse back to prior behavior where syncs are no-ops. This fixes a user regression where if a system is running a faulty fuse server that does not reply to issued write requests, this causes wait_sb_inodes() to wait forever.	N/A	More Details
CVE-2026-24135	Gogs is an open source self-hosted Git service. In version 0.13.3 and prior, a path traversal vulnerability exists in the updateWikiPage function of Gogs. The vulnerability allows an authenticated user with write access to a repository's wiki to delete arbitrary files on the server by manipulating the old_title parameter in the wiki editing form. This issue has been patched in versions 0.13.4 and 0.14.0+dev.	N/A	More Details
CVE-2026-23110	In the Linux kernel, the following vulnerability has been resolved: scsi: core: Wake up the error handler when final completions race against each other The fragile ordering between marking commands completed or failed so that the error handler only wakes when the last running command completes or times out has race conditions. These race conditions can cause the SCSI layer to fail to wake the error handler, leaving I/O through the SCSI host stuck as the error state cannot advance. First, there is an memory ordering issue within scsi_dec_host_busy(). The write which clears SCMD_STATE_INFLIGHT may be reordered with reads counting in scsi_host_busy(). While the local CPU will see its own write, reordering can allow other CPUs in scsi_dec_host_busy() or scsi_eh_inc_host_failed() to see a raised busy count, causing no CPU to see a host busy equal to the host_failed count. This race condition can be prevented with a memory barrier on the error path to force the write to be visible before counting host busy commands. Second, there is a general ordering issue with scsi_eh_inc_host_failed(). By counting busy commands before incrementing host_failed, it can race with a final command in scsi_dec_host_busy(), such that scsi_dec_host_busy() does not see host_failed incremented but scsi_eh_inc_host_failed() counts busy commands before SCMD_STATE_INFLIGHT is cleared by scsi_dec_host_busy(), resulting in neither waking the error handler task. This needs the call to scsi_host_busy() to be moved after host_failed is incremented to close the race condition.	N/A	More Details
CVE-2025-11004	The Simplicity Device Manager Tool has a Reflected XSS (Cross-site-scripting) vulnerability in several API endpoints. The attacker needs to be on the same network to execute this attack. These APIs can affect confidentiality, integrity, and availability of the system that has Simplicity Device Manager tool running in the background.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: netrom: fix double-free in		

CVE-2026-23098	In the Linux kernel, the following vulnerability has been resolved: netrom: fix double-free in nr_route_frame() In nr_route_frame(), old_skb is immediately freed without checking if nr_neigh->ax25 pointer is NULL. Therefore, if nr_neigh->ax25 is NULL, the caller function will free old_skb again, causing a double-free bug. Therefore, to prevent this, we need to modify it to check whether nr_neigh->ax25 is NULL before freeing old_skb.	N/A	More Details
CVE-2026-24903	OrcaStatLLM Researcher is an LLM Based Research Paper Generator. A Stored Cross-Site Scripting (XSS) vulnerability was discovered in the Log Message in the Session Page in OrcaStatLLM-Researcher that allows attackers to inject and execute arbitrary JavaScript code in victims' browsers through malicious research topic inputs.	N/A	More Details
CVE-2026-23097	In the Linux kernel, the following vulnerability has been resolved: migrate: correct lock ordering for hugetlb file folios Syzbot has found a deadlock (analyzed by Lance Yang): 1) Task (5749): Holds folio_lock, then tries to acquire i_mmap_rwsem(read lock). 2) Task (5754): Holds i_mmap_rwsem(write lock), then tries to acquire folio_lock. migrate_pages() -> migrate_hugetlbs() -> unmap_and_move_huge_page() <- Takes folio_lock! -> remove_migration_ptes() -> __rmap_walk_file() -> i_mmap_lock_read() <- Waits for i_mmap_rwsem(read lock)! hugetlbfs_fallocate() -> hugetlbfs_punch_hole() <- Takes i_mmap_rwsem(write lock)! -> hugetlbfs_zero_partial_page() -> filemap_lock_hugetlb_folio() -> filemap_lock_folio() -> __filemap_get_folio <- Waits for folio_lock! The migration path is the one taking locks in the wrong order according to the documentation at the top of mm/rmap.c. So expand the scope of the existing i_mmap_lock to cover the calls to remove_migration_ptes() too. This is (mostly) how it used to be after commit c0d0381ade79. That was removed by 336bf30eb765 for both file & anon hugetlb pages when it should only have been removed for anon hugetlb pages.	N/A	More Details
CVE-2026-23096	In the Linux kernel, the following vulnerability has been resolved: uacce: fix cdev handling in the cleanup path When cdev_device_add fails, it internally releases the cdev memory, and if cdev_device_del is then executed, it will cause a hang error. To fix it, we check the return value of cdev_device_add() and clear uacce->cdev to avoid calling cdev_device_del in the uacce_remove.	N/A	More Details
CVE-2026-0653	On TP-Link Tapo C260 v1, a guest-level authenticated user can bypass intended access restrictions by sending crafted requests to a synchronization endpoint. This allows modification of protected device settings despite limited privileges. An attacker may change sensitive configuration parameters without authorization, resulting in unauthorized device state manipulation but not full code execution.	N/A	More Details
CVE-2026-0652	On TP-Link Tapo C260 v1, command injection vulnerability exists due to improper sanitization in certain POST parameters during configuration synchronization. An authenticated attacker can execute arbitrary system commands with high impact on confidentiality, integrity and availability. It may cause full device compromise.	N/A	More Details
CVE-2026-0651	On TP-Link Tapo C260 v1, path traversal is possible due to improper handling of specific GET request paths via https, allowing local unauthenticated probing of filesystem paths. An attacker on the local network can determine whether certain files exists on the device, with no read, write or code execution possibilities.	N/A	More Details
CVE-2025-6010	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-24050	Zulip is an open-source team collaboration tool. From 5.0 to before 11.5, some administrative actions on the user profile were susceptible to stored XSS in group names or channel names. Exploiting these vulnerabilities required the user explicitly interacting with the problematic object. This vulnerability is fixed in 11.5.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: vsock/virtio: cap TX credit to local buffer size The virtio transports derives its TX credit directly from peer_buf_alloc, which is set from the remote endpoint's SO_VM_SOCKETS_BUFFER_SIZE value. On the host side this means that the amount of data we are willing to queue for a connection is scaled by a guest-chosen buffer size, rather than the host's own vsock configuration. A malicious guest can advertise a large buffer and read slowly, causing the host to allocate a correspondingly large amount of sk_buff memory. The same thing would happen in the guest with a malicious host, since virtio transports share the same code base. Introduce a		

CVE-2026-23086	guest with a malicious host, since virtio transports share the same code base. Introduce a small helper, virtio_transport_tx_buf_size(), that returns min(peer_buf_alloc, buf_alloc), and use it wherever we consume peer_buf_alloc. This ensures the effective TX window is bounded by both the peer's advertised buffer and our own buf_alloc (already clamped to buffer_max_size via SO_VM_SOCKETS_BUFFER_MAX_SIZE), so a remote peer cannot force the other to queue more data than allowed by its own vsock settings. On an unpatched Ubuntu 22.04 host (~64 GiB RAM), running a PoC with 32 guest vsock connections advertising 2 GiB each and reading slowly drove Slab/SUnreclaim from ~0.5 GiB to ~57 GiB; the system only recovered after killing the QEMU process. That said, if QEMU memory is limited with cgroups, the maximum memory used will be limited. With this patch applied: Before: MemFree: ~61.6 GiB Slab: ~142 MiB SUnreclaim: ~117 MiB After 32 high-credit connections: MemFree: ~61.5 GiB Slab: ~178 MiB SUnreclaim: ~152 MiB Only ~35 MiB increase in Slab/SUnreclaim, no host OOM, and the guest remains responsive. Compatibility with non-virtio transports: - VMCI uses the AF_VSOCK buffer knobs to size its queue pairs per socket based on the local vsk->buffer_* values; the remote side cannot enlarge those queues beyond what the local endpoint configured. - Hyper-V's vsock transport uses fixed-size VMBus ring buffers and an MTU bound; there is no peer-controlled credit field comparable to peer_buf_alloc, and the remote endpoint cannot drive in-flight kernel memory above those ring sizes. - The loopback path reuses virtio_transport_common.c, so it naturally follows the same semantics as the virtio transport. This change is limited to virtio_transport_common.c and thus affects virtio-vsock, vhost-vsock, and loopback, bringing them in line with the "remote window intersected with local policy" behaviour that VMCI and Hyper-V already effectively have. [Stefano: small adjustments after changing the previous patch] [Stefano: tweak the commit message]	N/A	More Details
CVE-2026-23087	In the Linux kernel, the following vulnerability has been resolved: scsi: xen: scsiback: Fix potential memory leak in scsiback_remove() Memory allocated for struct vscsiblk_info in scsiback_probe() is not freed in scsiback_remove() leading to potential memory leaks on remove, as well as in the scsiback_probe() error paths. Fix that by freeing it in scsiback_remove().	N/A	More Details
CVE-2026-23088	In the Linux kernel, the following vulnerability has been resolved: tracing: Fix crash on synthetic stacktrace field usage When creating a synthetic event based on an existing synthetic event that had a stacktrace field and the new synthetic event used that field a kernel crash occurred: ~# cd /sys/kernel/tracing ~# echo 's:stack unsigned long stack[];' > dynamic_events ~# echo 'hist:keys=prev_pid:s0=common_stacktrace if prev_state & 3' >> events/sched/sched_switch/trigger ~# echo 'hist:keys=next_pid:s1=$s0:onmatch(sched.sched_switch).trace(stack,$s1)' >> events/sched/sched_switch/trigger The above creates a synthetic event that takes a stacktrace when a task schedules out in a non-running state and passes that stacktrace to the sched_switch event when that task schedules back in. It triggers the "stack" synthetic event that has a stacktrace as its field (called "stack"). ~# echo 's:syscall_stack s64 id; unsigned long stack[];' >> dynamic_events ~# echo 'hist:keys=common_pid:s2=stack' >> events/synthetic/stack/trigger ~# echo 'hist:keys=common_pid:s3=$s2,i0=id:onmatch(synthetic.stack).trace(syscall_stack,$i0,$s3)' >> events/raw_syscalls/sys_exit/trigger The above makes another synthetic event called "syscall_stack" that attaches the first synthetic event (stack) to the sys_exit trace event and records the stacktrace from the stack event with the id of the system call that is exiting. When enabling this event (or using it in a historgram): ~# echo 1 > events/synthetic/syscall_stack/enable Produces a kernel crash! BUG: unable to handle page fault for address: 0000000000400010 #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: 6 UID: 0 PID: 1257 Comm: bash Not tainted 6.16.3+deb14-amd64 #1 PREEMPT(lazy) Debian 6.16.3-1 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.17.0-debian-1.17.0-1 04/01/2014 RIP: 0010:trace_event_raw_event_synth+0x90/0x380 Code: c5 00 00 00 00 85 d2 0f 84 e1 00 00 00 31 db eb 34 0f 1f 00 66 66 2e 0f 1f 84 00 00 00 00 00 66 66 2e 0f 1f 84 00 00 00 00 00 <49> 8b 04 24 48 83 c3 01 8d 0c c5 08 00 00 00 01 cd 41 3b 5d 40 0f RSP: 0018:ffffd2670388f958 EFLAGS: 00010202 RAX: ffff8ba1065cc100 RBX: 0000000000000000 RCX: 0000000000000000 RDX: 0000000000000001 RSI: fffff266ffda7b90 RDI: ffffd2670388f9b0 RBP: 0000000000000010 R08: ffff8ba104e76000 R09: ffffd2670388fa50 R10: ffff8ba102dd42e0 R11: ffffffff9a908970 R12: 0000000000400010 R13: ffff8ba10a246400 R14: ffff8ba10a710220 R15: fffff266ffda7b90 FS: 00007fa3bc63f740(0000) GS:ffff8ba2e0f48000(0000) knlGS:0000000000000000 CS:	N/A	More Details

	0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000400010 CR3: 0000000107f9e003 CR4: 0000000000172ef0 Call Trace: <TASK> ? __tracing_map_insert+0x208/0x3a0 action_trace+0x67/0x70 event_hist_trigger+0x633/0x6d0 event_triggers_call+0x82/0x130 trace_event_buffer_commit+0x19d/0x250 trace_event_raw_event_sys_exit+0x62/0xb0 syscall_exit_work+0x9d/0x140 do_syscall_64+0x20a/0x2f0 ? trace_event_raw_event_sched_switch+0x12b/0x170 ? save_fpregs_to_fpstate+0x3e/0x90 ? _raw_spin_unlock+0xe/0x30 ? finish_task_switch.isra.0+0x97/0x2c0 ? __rseq_handle_notify_resume+0xad/0x4c0 ? __schedule+0x4b8/0xd00 ? restore_fpregs_from_fpstate+0x3c/0x90 ? switch_fpu_return+0x5b/0xe0 ? do_syscall_64+0x1ef/0x2f0 ? do_fault+0x2e9/0x540 ? __handle_mm_fault+0x7d1/0xf70 ? count_memcg_events+0x167/0x1d0 ? handle_mm_fault+0x1d7/0x2e0 ? do_user_addr_fault+0x2c3/0x7f0 entry_SYSCALL_64_after_hwframe+0x76/0x7e The reason is that the stacktrace field is not labeled as such, and is treated as a normal field and not as a dynamic event that it is. In trace_event_raw_event_synth() the event is field is still treated as a dynamic array, but the retrieval of the data is considered a normal field, and the reference is just the meta data: // Meta data is retrieved instead of a dynamic array --- truncated---		
CVE-2026-23089	In the Linux kernel, the following vulnerability has been resolved: ALSA: usb-audio: Fix use-after-free in snd_usb_mixer_free() When snd_usb_create_mixer() fails, snd_usb_mixer_free() frees mixer->id_elems but the controls already added to the card still reference the freed memory. Later when snd_card_register() runs, the OSS mixer layer calls their callbacks and hits a use-after-free read. Call trace: get_ctl_value+0x63f/0x820 sound/usb/mixer.c:411 get_min_max_with_quirks.isra.0+0x240/0x1f40 sound/usb/mixer.c:1241 mixer_ctl_feature_info+0x26b/0x490 sound/usb/mixer.c:1381 snd_mixer_oss_build_test+0x174/0x3a0 sound/core/oss/mixer_oss.c:887 ... snd_card_register+0x4ed/0x6d0 sound/core/init.c:923 usb_audio_probe+0x5ef/0x2a90 sound/usb/card.c:1025 Fix by calling snd_ctl_remove() for all mixer controls before freeing id_elems. We save the next pointer first because snd_ctl_remove() frees the current element.	N/A	More Details
CVE-2026-23090	In the Linux kernel, the following vulnerability has been resolved: slimbus: core: fix device reference leak on report present Slimbus devices can be allocated dynamically upon reception of report-present messages. Make sure to drop the reference taken when looking up already registered devices. Note that this requires taking an extra reference in case the device has not yet been registered and has to be allocated.	N/A	More Details
CVE-2026-23091	In the Linux kernel, the following vulnerability has been resolved: intel_th: fix device leak on output open() Make sure to drop the reference taken when looking up the th device during output device open() on errors and on close(). Note that a recent commit fixed the leak in a couple of open() error paths but not all of them, and the reference is still leaking on successful open().	N/A	More Details
CVE-2026-23092	In the Linux kernel, the following vulnerability has been resolved: iio: dac: ad3552r-hs: fix out-of-bound write in ad3552r_hs_write_data_source When simple_write_to_buffer() succeeds, it returns the number of bytes actually copied to the buffer. The code incorrectly uses 'count' as the index for null termination instead of the actual bytes copied. If count exceeds the buffer size, this leads to out-of-bounds write. Add a check for the count and use the return value as the index. The bug was validated using a demo module that mirrors the original code and was tested under QEMU. Pattern of the bug: - A fixed 64-byte stack buffer is filled using count. - If count > 64, the code still does buf[count] = '\0', causing an - out-of-bounds write on the stack. Steps for reproduce: - Opens the device node. - Writes 128 bytes of A to it. - This overflows the 64-byte stack buffer and KASAN reports the OOB. Found via static analysis. This is similar to the commit da9374819eb3 ("iio: backend: fix out-of-bound write")	N/A	More Details
CVE-2026-23093	In the Linux kernel, the following vulnerability has been resolved: ksmbd: smbd: fix dma_unmap_sg() nents The dma_unmap_sg() functions should be called with the same nents as the dma_map_sg(), not the value the map function returned.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: uacce: fix isolate sysfs check condition uacce supports the device isolation feature. If the driver implements the		

CVE-2026-23094	check condition uacce supports the device isolation feature. If the driver implements the isolate_err_threshold_read and isolate_err_threshold_write callback functions, uacce will create sysfs files now. Users can read and configure the isolation policy through sysfs. Currently, sysfs files are created as long as either isolate_err_threshold_read or isolate_err_threshold_write callback functions are present. However, accessing a non-existent callback function may cause the system to crash. Therefore, intercept the creation of sysfs if neither read nor write exists; create sysfs if either is supported, but intercept unsupported operations at the call site.	N/A	More Details
CVE-2026-23095	In the Linux kernel, the following vulnerability has been resolved: gue: Fix skb memleak with inner IP protocol 0. syzbot reported skb memleak below. [0] The repro generated a GUE packet with its inner protocol 0. gue_udp_recv() returns -guehdr->proto_ctype for "resubmit" in ip_protocol_deliver_rcu(), but this only works with non-zero protocol number. Let's drop such packets. Note that 0 is a valid number (IPv6 Hop-by-Hop Option). I think it is not practical to encap HOPOPT in GUE, so once someone starts to complain, we could pass down a resubmit flag pointer to distinguish two zeros from the upper layer: * no error * resubmit HOPOPT [0] BUG: memory leak unreferenced object 0xffff888109695a00 (size 240): comm "syz.0.17", pid 6088, jiffies 4294943096 hex dump (first 32 bytes): 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 00 40 c2 10 81 88 ff ff 00 00 00 00 00 00 00 00 .@..... backtrace (crc a84b336f): kmemleak_alloc_recursive include/linux/kmemleak.h:44 [inline] slab_post_alloc_hook mm/slub.c:4958 [inline] slab_alloc_node mm/slub.c:5263 [inline] kmem_cache_alloc_noprof+0x3b4/0x590 mm/slub.c:5270 __build_skb+0x23/0x60 net/core/skbuff.c:474 build_skb+0x20/0x190 net/core/skbuff.c:490 __tun_build_skb drivers/net/tun.c:1541 [inline] tun_build_skb+0x4a1/0xa40 drivers/net/tun.c:1636 tun_get_user+0xc12/0x2030 drivers/net/tun.c:1770 tun_chr_write_iter+0x71/0x120 drivers/net/tun.c:1999 new_sync_write fs/read_write.c:593 [inline] vfs_write+0x45d/0x710 fs/read_write.c:686 ksys_write+0xa7/0x170 fs/read_write.c:738 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xa4/0xf80 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f	N/A	More Details
CVE-2025-64175	Gogs is an open source self-hosted Git service. In version 0.13.3 and prior, Gogs' 2FA recovery code validation does not scope codes by user, enabling cross-account bypass. If an attacker knows a victim's username and password, they can use any unused recovery code (e.g., from their own account) to bypass the victim's 2FA. This enables full account takeover and renders 2FA ineffective in all environments where it's enabled.. This issue has been patched in versions 0.13.4 and 0.14.0+dev.	N/A	More Details
CVE-2025-69213	OpenSTAManager is an open source management software for technical assistance and invoicing. In version 2.9.8 and prior, a SQL Injection vulnerability exists in the ajax_complete.php endpoint when handling the get_sedi operation. An authenticated attacker can inject malicious SQL code through the idanagrafica parameter, leading to unauthorized database access. At time of publication, no known patch exists.	N/A	More Details
CVE-2026-25556	MuPDF versions 1.23.0 through 1.27.0 contain a double-free vulnerability in fz_fill_pixmap_from_display_list() when an exception occurs during display list rendering. The function accepts a caller-owned fz_pixmap pointer but incorrectly drops the pixmap in its error handling path before rethrowing the exception. Callers (including the barcode decoding path in fz_decode_barcode_from_display_list) also drop the same pixmap in cleanup, resulting in a double-free that can corrupt the heap and crash the process. This issue affects applications that enable and use MuPDF barcode decoding and can be triggered by processing crafted input that causes a rendering-time error while decoding barcodes.	N/A	More Details
CVE-2026-25973	Rejected reason: Not used	N/A	More Details
CVE-2026-25857	Tenda G300-F router firmware version 16.01.14.2 and prior contain an OS command injection vulnerability in the WAN diagnostic functionality (formSetWanDiag). The implementation constructs a shell command that invokes curl and incorporates attacker-controlled input into the command line without adequate neutralization. As a result, a remote attacker with access to the affected management interface can inject additional	N/A	More Details

	shell syntax and execute arbitrary commands on the device with the privileges of the management process.		
CVE-2026-25858	macrozheng mall version 1.0.3 and prior contains an authentication vulnerability in the mall-portal password reset workflow that allows an unauthenticated attacker to reset arbitrary user account passwords using only a victim's telephone number. The password reset flow exposes the one-time password (OTP) directly in the API response and validates password reset requests solely by comparing the provided OTP to a value stored by telephone number, without verifying user identity or ownership of the telephone number. This enables remote account takeover of any user with a known or guessable telephone number.	N/A	More Details
CVE-2026-25499	Terraform / OpenTofu Provider adds support for Proxmox Virtual Environment. Prior to version 0.93.1, in the SSH configuration documentation, the sudoer line suggested is insecure and can result in escaping the folder using ../, allowing any files on the system to be edited. This issue has been patched in version 0.93.1.	N/A	More Details
CVE-2026-25511	Group-Office is an enterprise customer relationship management and groupware tool. Prior to versions 6.8.150, 25.0.82, and 26.0.5, an authenticated user within the System Administrator group can trigger a full SSRF via the WOPI service discovery URL, including access to internal hosts/ports. The SSRF response body can be exfiltrated via the built-in debug system, turning it into a visible SSRF. This also allows full server-side file read. This issue has been patched in versions 6.8.150, 25.0.82, and 26.0.5.	N/A	More Details
CVE-2026-25512	Group-Office is an enterprise customer relationship management and groupware tool. Prior to versions 6.8.150, 25.0.82, and 26.0.5, there is a remote code execution (RCE) vulnerability in Group-Office. The endpoint email/message/tnefAttachmentFromTempFile directly concatenates the user-controlled parameter tmp_file into an exec() call. By injecting shell metacharacters into tmp_file, an authenticated attacker can execute arbitrary system commands on the server. This issue has been patched in versions 6.8.150, 25.0.82, and 26.0.5.	N/A	More Details
CVE-2026-25517	Wagtail is an open source content management system built on Django. Prior to versions 6.3.6, 7.0.4, 7.1.3, 7.2.2, and 7.3, due to a missing permission check on the preview endpoints, a user with access to the Wagtail admin and knowledge of a model's fields can craft a form submission to obtain a preview rendering of any page, snippet or site setting object for which previews are enabled, consisting of any data of the user's choosing. The existing data of the object itself is not exposed, but depending on the nature of the template being rendered, this may expose other database contents that would otherwise only be accessible to users with edit access over the model. The vulnerability is not exploitable by an ordinary site visitor without access to the Wagtail admin. This issue has been patched in versions 6.3.6, 7.0.4, 7.1.3, 7.2.2, and 7.3.	N/A	More Details
CVE-2026-25951	FUXA is a web-based Process Visualization (SCADA/HMI/Dashboard) software. Prior to 1.2.11, there is a flaw in the path sanitization logic allows an authenticated attacker with administrative privileges to bypass directory traversal protections. By using nested traversal sequences (e.g., .../), an attacker can write arbitrary files to the server filesystem, including sensitive directories like runtime/scripts. This leads to Remote Code Execution (RCE) when the server reloads the malicious scripts. This vulnerability is fixed in 1.2.11.	N/A	More Details
CVE-2026-25939	FUXA is a web-based Process Visualization (SCADA/HMI/Dashboard) software. From 1.2.8 through version 1.2.10, an authorization bypass vulnerability in the FUXA allows an unauthenticated, remote attacker to create and modify arbitrary schedulers, exposing connected ICS/SCADA environments to follow-on actions. This has been patched in FUXA version 1.2.11.	N/A	More Details
CVE-2026-25938	FUXA is a web-based Process Visualization (SCADA/HMI/Dashboard) software. From 1.2.8 through 1.2.10, an authentication bypass vulnerability in FUXA allows an unauthenticated, remote attacker to execute arbitrary code on the server when the Node-RED plugin is enabled. This has been patched in FUXA version 1.2.11.	N/A	More Details
CVE-2026-	FUXA is a web-based Process Visualization (SCADA/HMI/Dashboard) software. A path traversal vulnerability in FUXA allows an unauthenticated, remote attacker to write arbitrary files to arbitrary locations on the server filesystem. This affects FUXA through version 1.2.9.	N/A	More Details

25895	This issue has been patched in FUXA version 1.2.10.		
CVE-2026-25894	FUXA is a web-based Process Visualization (SCADA/HMI/Dashboard) software. An insecure default configuration in FUXA allows an unauthenticated, remote attacker to gain administrative access and execute arbitrary code on the server. This affects FUXA through version 1.2.9 when authentication is enabled, but the administrator JWT secret is not configured. This issue has been patched in FUXA version 1.2.10.	N/A	More Details
CVE-2026-25893	FUXA is a web-based Process Visualization (SCADA/HMI/Dashboard) software. Prior to 1.2.10, an authentication bypass vulnerability in FUXA allows an unauthenticated, remote attacker to gain administrative access via the heartbeat refresh API and execute arbitrary code on the server. This issue has been patched in FUXA version 1.2.10.	N/A	More Details
CVE-2026-25521	Locutus brings stdlibs of other programming languages to JavaScript for educational purposes. In versions from 2.0.12 to before 2.0.39, a prototype pollution vulnerability exists in locutus. Despite a previous fix that attempted to mitigate prototype pollution by checking whether user input contained a forbidden key, it is still possible to pollute Object.prototype via a crafted input using String.prototype. This issue has been patched in version 2.0.39.	N/A	More Details
CVE-2026-25793	Nebula is a scalable overlay networking tool. In versions from 1.7.0 to 1.10.2, when using P256 certificates (which is not the default configuration), it is possible to evade a blocklist entry created against the fingerprint of a certificate by using ECDSA Signature Malleability to use a copy of the certificate with a different fingerprint. This issue has been patched in version 1.10.3.	N/A	More Details
CVE-2026-25537	jsonwebtoken is a JWT lib in rust. Prior to version 10.3.0, there is a Type Confusion vulnerability in jsonwebtoken, specifically, in its claim validation logic. When a standard claim (such as nbf or exp) is provided with an incorrect JSON type (Like a String instead of a Number), the library's internal parsing mechanism marks the claim as "FailedToParse". Crucially, the validation logic treats this "FailedToParse" state identically to "NotPresent". This means that if a check is enabled (like: validate_nbf = true), but the claim is not explicitly marked as required in required_spec_claims, the library will skip the validation check entirely for the malformed claim, treating it as if it were not there. This allows attackers to bypass critical time-based security restrictions (like "Not Before" checks) and commit potential authentication and authorization bypasses. This issue has been patched in version 10.3.0.	N/A	More Details
CVE-2026-0945	Privilege Defined With Unsafe Actions vulnerability in Drupal Role Delegation allows Privilege Escalation.This issue affects Role Delegation: from 1.3.0 before 1.5.0.	N/A	More Details
CVE-2026-25974	Rejected reason: Not used	N/A	More Details
CVE-2025-69215	OpenSTAManager is an open source management software for technical assistance and invoicing. In version 2.9.8 and prior, there is a SQL Injection vulnerability in the Stampe Module. At time of publication, no known patch exists.	N/A	More Details
CVE-2026-25975	Rejected reason: Not used	N/A	More Details
CVE-2026-21893	n8n is an open source workflow automation platform. From version 0.187.0 to before 1.120.3, a command injection vulnerability was identified in n8n's community package installation functionality. The issue allowed authenticated users with administrative permissions to execute arbitrary system commands on the n8n host under specific conditions. This issue has been patched in version 1.120.3.	N/A	More Details
CVE-2026-	RIOT is an open-source microcontroller operating system, designed to match the requirements of Internet of Things (IoT) devices and other embedded devices. In version 2025.10 and prior, multiple out-of-bounds read allow any unauthenticated user, with ability to send or manipulate input packets, to read adjacent memory locations, or crash a	N/A	More Details

25139	vulnerable device running the 6LoWPAN stack. The received packet is cast into a sixlowpan_sfr_rfrag_t struct and dereferenced without validating the packet is large enough to contain the struct object. At time of publication, no known patch exists.		
CVE-2026-23901	Observable Timing Discrepancy vulnerability in Apache Shiro. This issue affects Apache Shiro: from 1.*, 2.* before 2.0.7. Users are recommended to upgrade to version 2.0.7 or later, which fixes the issue. Prior to Shiro 2.0.7, code paths for non-existent vs. existing users are different enough, that a brute-force attack may be able to tell, by timing the requests only, determine if the request failed because of a non-existent user vs. wrong password. The most likely attack vector is a local attack only. Shiro security model https://shiro.apache.org/security-model.html#username_enumeration discusses this as well. Typically, brute force attack can be mitigated at the infrastructure level.	N/A	More Details
CVE-2026-25481	Langroid is a framework for building large-language-model-powered applications. Prior to version 0.59.32, there is a bypass to the fix for CVE-2025-46724. TableChatAgent can call pandas_eval tool to evaluate the expression. There is a WAF in langroid/utils/pandas_utils.py introduced to block code injection CVE-2025-46724. However it can be bypassed due to _literal_ok() returning False instead of raising UnsafeCommandError on invalid input, combined with unrestricted access to dangerous dunder attributes (__init__, __globals__, __builtins__). This allows chaining whitelisted DataFrame methods to leak the eval builtin and execute arbitrary code. This issue has been patched in version 0.59.32.	N/A	More Details
CVE-2026-25513	FacturaScripts is open-source enterprise resource planning and accounting software. Prior to version 2025.81, FacturaScripts contains a critical SQL injection vulnerability in the REST API that allows authenticated API users to execute arbitrary SQL queries through the sort parameter. The vulnerability exists in the ModelClass::getOrderBy() method where user-supplied sorting parameters are directly concatenated into the SQL ORDER BY clause without validation or sanitization. This affects all API endpoints that support sorting functionality. This issue has been patched in version 2025.81.	N/A	More Details
CVE-2026-25514	FacturaScripts is open-source enterprise resource planning and accounting software. Prior to version 2025.81, FacturaScripts contains a critical SQL injection vulnerability in the autocomplete functionality that allows authenticated attackers to extract sensitive data from the database including user credentials, configuration settings, and all stored business data. The vulnerability exists in the CodeModel::all() method where user-supplied parameters are directly concatenated into SQL queries without sanitization or parameterized binding. This issue has been patched in version 2025.81.	N/A	More Details
CVE-2026-1337	Insufficient escaping of unicode characters in query log in Neo4j Enterprise and Community editions prior to 2026.01 can lead to XSS if the user opens the logs in a tool that treats them as HTML. There is no security impact on Neo4j products, but this advisory is released as a precaution to treat the logs as plain text if using versions prior to 2026.01. Proof of concept exploit: https://github.com/JoakimBulow/CVE-2026-1337	N/A	More Details
CVE-2025-13818	Local privilege escalation vulnerability via insecure temporary batch file execution in ESET Management Agent	N/A	More Details
CVE-2026-25566	WeKan versions prior to 8.19 contain an authorization vulnerability in card move logic. A user can specify a destination board/list/swimlane without adequate authorization checks for the destination and without validating that destination objects belong to the destination board, potentially enabling unauthorized cross-board moves.	N/A	More Details
CVE-2026-25981	Rejected reason: Not used	N/A	More Details
CVE-2026-25980	Rejected reason: Not used	N/A	More Details
CVE-2026-25979	Rejected reason: Not used	N/A	More Details

CVE-2026-25978	Rejected reason: Not used	N/A	More Details
CVE-2026-25977	Rejected reason: Not used	N/A	More Details
CVE-2026-25976	Rejected reason: Not used	N/A	More Details
CVE-2026-25804	Antrea is a Kubernetes networking solution intended to be Kubernetes native. Prior to versions 2.3.2 and 2.4.3, Antrea's network policy priority assignment system has a uint16 arithmetic overflow bug that causes incorrect OpenFlow priority calculations when handling a large numbers of policies with various priority values. This results in potentially incorrect traffic enforcement. This issue has been patched in versions 2.4.3.	N/A	More Details