SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 24 June 2026

Generated on 24 June 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-2026-10561	IBM Langflow OSS 1.0.0 through 1.9.3 has an vulnerability due to an improper isolation of Python execution combined with an authentication bypass that allows an unauthenticated attacker to execute arbitrary code on the host system, resulting in complete compromise	10.0	More Details
CVE-2026-49257	mcp-pinot is a Python-based Model Context Protocol (MCP) server for interacting with Apache Pinot. In versions 3.0.1 and below, mcp-pinot defaults to running an HTTP MCP server bound to 0.0.0.0:8080 with no authentication enabled. All MCP tools, including SQL query execution, schema creation, and table-config mutation, are reachable by any network-adjacent caller. The server proxies these calls using server-side Pinot credentials, producing a confused-deputy condition that yields full read/write access to the configured Pinot cluster. This issue has been fixed in version 3.1.0	10.0	More Details
CVE-2026-48772	ProxySQL is a proxy for MySQL and its forks, as well as PostgreSQL. In versions 2.0.0 through 3.0.8, the ProxySQL MySQL frontend accepts the `PROXY UNKNOWN <addr> <addr> <port> <port>\r\n` PP1 frame as a well-formed PROXY protocol header. The HAProxy PROXY protocol v1 specification says that when the protocol token is `UNKNOWN`, the receiver MUST ignore any address fields that follow it, because the proxy has declared it cannot determine the client identity. ProxySQL parses those address fields anyway via `sscanf` and writes the spoofed source address into the session's `addr.addr` field. From there it flows directly into the query-rule matcher, where the `client_addr` predicate decides routing and ACL. When `mysql-proxy_protocol_networks = '*'` (the default), any TCP peer can send a PP1 frame and choose any source IP claim. With that, any `mysql_query_rules` row pinned to a `client_addr` value is forgeable: the attacker writes the address they want to match into the PP1 line, and ProxySQL routes their query as if it came from that address. In practice this is a routing and ACL bypass. Real deployments use `client_addr` for read-write splitting (internal apps go to the primary, public traffic to read replicas), per-app schema pinning, and query-filter rules (DDL allowed only from admin CIDR, public queries blocked from dangerous patterns). An attacker that can reach the frontend port can forge their way into any of those routes. Version 3.0.9 patches this issue.	10.0	More Details

CVE-2026-46778	Vulnerability in the Oracle WebCenter Enterprise Capture product of Oracle Fusion Middleware (component: Client Bundle). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via RMI to compromise Oracle WebCenter Enterprise Capture. While the vulnerability is in Oracle WebCenter Enterprise Capture, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Enterprise Capture. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).	10.0	More Details
CVE-2026-50242	In JetBrains Hub before 2026.1.13757, 2025.3.148033, 2025.2.148048, 2025.1.148120, 2024.3.148430, 2024.2.148429 authentication bypass via direct database access leading to administrative access was possible	10.0	More Details
CVE-2026-46803	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Security Framework). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Portal. While the vulnerability is in Oracle WebCenter Portal, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Portal. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).	10.0	More Details
CVE-2026-46781	Vulnerability in the Oracle WebCenter Enterprise Capture product of Oracle Fusion Middleware (component: Client Bundle). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via RMI to compromise Oracle WebCenter Enterprise Capture. While the vulnerability is in Oracle WebCenter Enterprise Capture, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Enterprise Capture. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).	10.0	More Details
CVE-2026-46978	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Remote Administration Daemon). The supported version that is affected is 11.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Solaris. While the vulnerability is in Oracle Solaris, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Solaris accessible data as well as unauthorized access to critical data or complete access to all Oracle Solaris accessible data. CVSS 3.1 Base Score 10.0 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N).	10.0	More Details
CVE-2025-69129	Unauthenticated Arbitrary File Upload in WordPress & WooCommerce Scraper Plugin, Import Data from Any Site <= 1.0.7 versions.	10.0	More Details
CVE-2026-35308	Vulnerability in the Oracle Coherence product of Oracle Fusion Middleware (component: Centralized Third Party Jars). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0 and 15.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Coherence. While the vulnerability is in Oracle Coherence, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Coherence. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).	10.0	More Details
CVE-2026-35307	Vulnerability in the Oracle Coherence product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0 and 15.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Coherence. While the vulnerability is in Oracle Coherence, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Coherence. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).	10.0	More Details
CVE-2026-25470	Improper Control of Generation of Code ('Code Injection') vulnerability in ACPT ACPT (Pro) - Custom Post Types Plugin for WordPress allows Remote Code Inclusion. This issue affects ACPT (Pro) - Custom Post Types Plugin for WordPress: from n/a through 2.0.47.	10.0	More Details

CVE-2026-35301	Vulnerability in the WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise WebLogic Server. While the vulnerability is in WebLogic Server, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of WebLogic Server. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).	10.0	More Details
CVE-2026-45480	Improper authentication in Azure Active Directory allows an unauthorized attacker to elevate privileges over a network.	10.0	More Details
CVE-2026-3490	picklescan before 1.0.4 fails to block pkgutil.resolve_name, allowing attackers to bypass the entire blocklist by resolving any dangerous function through indirect REDUCE calls. Remote attackers can invoke any blocked function such as os.system, builtins.exec, or subprocess.call to achieve remote code execution.	10.0	More Details
CVE-2026-35292	Vulnerability in the WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 14.1.2.0.0 and 15.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise WebLogic Server. While the vulnerability is in WebLogic Server, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of WebLogic Server. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).	10.0	More Details
CVE-2026-46800	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Sites. While the vulnerability is in Oracle WebCenter Sites, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Sites. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).	10.0	More Details
CVE-2026-46846	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Security Framework). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Portal. While the vulnerability is in Oracle WebCenter Portal, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Portal. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).	10.0	More Details
CVE-2026-48055	Streambert is a cross-platform Electron Desktop App to stream and download any video media. In versions 2.4.0 and prior, a high-severity Zip Slip vulnerability was identified in Streambert's subtitle extraction logic. The application does not sanitize archive entry filenames during extraction, allowing a malicious archive to perform path traversal and write arbitrary files to the host filesystem. The subtitle extraction process downloads a ZIP archive and extracts its entries. The destination file path is constructed by concatenating the raw archive entry name (extracted.name) directly to the temporary directory path. If a malicious ZIP archive containing directory traversal sequences is processed, it escapes the temporary directory boundaries. The application then writes the extracted payload anywhere on the host filesystem subject to the application's current write permissions. This issue has been fixed in version 2.5.0.	10.0	More Details
CVE-2026-46798	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Sites. While the vulnerability is in Oracle WebCenter Sites, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Sites. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).	10.0	More Details

CVE-2026-46897	Vulnerability in the Oracle Enterprise Command Center Framework product of Oracle E-Business Suite (component: Core). Supported versions that are affected are V15 and V16. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Enterprise Command Center Framework. While the vulnerability is in Oracle Enterprise Command Center Framework, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Enterprise Command Center Framework accessible data as well as unauthorized access to critical data or complete access to all Oracle Enterprise Command Center Framework accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Enterprise Command Center Framework. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:L).	9.9	More Details
CVE-2026-46901	Vulnerability in the Oracle Enterprise Command Center Framework product of Oracle E-Business Suite (component: Core). Supported versions that are affected are V15 and V16. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Enterprise Command Center Framework. While the vulnerability is in Oracle Enterprise Command Center Framework, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Enterprise Command Center Framework accessible data as well as unauthorized access to critical data or complete access to all Oracle Enterprise Command Center Framework accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Enterprise Command Center Framework. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:L).	9.9	More Details
CVE-2026-46814	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Security Framework). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Portal. While the vulnerability is in Oracle WebCenter Portal, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Portal. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2026-46900	Vulnerability in the Oracle Enterprise Command Center Framework product of Oracle E-Business Suite (component: Core). Supported versions that are affected are V15 and V16. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise Oracle Enterprise Command Center Framework. While the vulnerability is in Oracle Enterprise Command Center Framework, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Command Center Framework. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2026-46832	Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Discovery Framework). Supported versions that are affected are 13.5 and 24.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise Oracle Enterprise Manager Base Platform. While the vulnerability is in Oracle Enterprise Manager Base Platform, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Manager Base Platform. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2026-46847	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Runtime Tools). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise Oracle WebCenter Portal. While the vulnerability is in Oracle WebCenter Portal, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Portal. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
	Vulnerability in the MySQL Shell product of Oracle MySQL (component: Shell for VS Code). The supported version that is affected is 2026.2.0+9.6.1. Easily exploitable vulnerability allows		

CVE-2026-46850	low privileged attacker with network access via HTTP to compromise MySQL Shell. While the vulnerability is in MySQL Shell, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of MySQL Shell. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2026-46838	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Security Framework). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise Oracle WebCenter Portal. While the vulnerability is in Oracle WebCenter Portal, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Portal. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2026-46844	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Security Framework). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise Oracle WebCenter Portal. While the vulnerability is in Oracle WebCenter Portal, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Portal. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2026-46893	Vulnerability in the JD Edwards EnterpriseOne General Ledger product of Oracle JD Edwards (component: E1 Foundation). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via SMB to compromise JD Edwards EnterpriseOne General Ledger. While the vulnerability is in JD Edwards EnterpriseOne General Ledger, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of JD Edwards EnterpriseOne General Ledger. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2026-46855	Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Metadata Plugin). Supported versions that are affected are 13.5 and 24.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise Oracle Enterprise Manager Base Platform. While the vulnerability is in Oracle Enterprise Manager Base Platform, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Manager Base Platform. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2026-46907	Vulnerability in the JD Edwards EnterpriseOne Order Promising product of Oracle JD Edwards (component: Order Promising Integration). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Order Promising. While the vulnerability is in JD Edwards EnterpriseOne Order Promising, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of JD Edwards EnterpriseOne Order Promising. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2026-46854	Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Target Management). Supported versions that are affected are 13.5 and 24.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Enterprise Manager Base Platform. While the vulnerability is in Oracle Enterprise Manager Base Platform, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Manager Base Platform. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2026-46852	Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Metadata Plugin). Supported versions that are affected are 13.5 and 24.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise Oracle Enterprise Manager Base Platform. While the vulnerability is in Oracle Enterprise Manager Base Platform, attacks may significantly impact additional	9.9	More Details

	products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Manager Base Platform. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).		
CVE-2026-46895	Vulnerability in the Oracle Enterprise Command Center Framework product of Oracle E-Business Suite (component: Core). Supported versions that are affected are V15 and V16. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Enterprise Command Center Framework. While the vulnerability is in Oracle Enterprise Command Center Framework, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Command Center Framework. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2026-35263	Vulnerability in the WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 14.1.2.0.0 and 15.1.1.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise WebLogic Server. While the vulnerability is in WebLogic Server, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of WebLogic Server. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2026-46908	Vulnerability in the JD Edwards EnterpriseOne Accounts Payable product of Oracle JD Edwards (component: Accounts Payable). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Accounts Payable. While the vulnerability is in JD Edwards EnterpriseOne Accounts Payable, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of JD Edwards EnterpriseOne Accounts Payable. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2026-47647	Improper access control in Microsoft Dynamics 365 allows an authorized attacker to elevate privileges over a network.	9.9	More Details
CVE-2026-48781	Postiz is an AI social media scheduling tool. In versions prior to 2.21.8, the Skool integration callback signed an attacker-controlled JSON blob into a session-shape JWT using the application's JWT_SECRET, and the auth middleware trusted every claim in that JWT without re-resolving the user from the database. Any authenticated Postiz user could forge a SUPERADMIN session and impersonate arbitrary organizations. This allowed Full Access to the following: all parts of Postiz, including users registered to the specific instance and the ability to post in the name of the victim's social media channels added to that Postiz instance. This issue has been fixed in version 2.21.8.	9.9	More Details
CVE-2026-49252	deepstream is a server that allows clients and backend services to sync data, send messages and make rpcs at scale. Versions prior to 10.0.5 are vulnerable to Prototype Pollution. Exploitation can lead to potential privilege escalation from any authenticated user with write permission to any record. This issue has been fixed in version 10.0.5.	9.9	More Details
CVE-2026-40783	Contributor Remote Code Execution (RCE) in Blocksy Companion Pro <= 2.1.37 versions.	9.9	More Details
CVE-2026-40749	Subscriber Arbitrary File Upload in Charity Zone <= 1.1.1 versions.	9.9	More Details
CVE-2026-40748	Subscriber Arbitrary File Upload in Kids Gift Shop <= 0.5.4 versions.	9.9	More Details
CVE-2026-40747	Subscriber Arbitrary File Upload in Ecommerce Zone <= 0.9.7 versions.	9.9	More Details
CVE-2026-40746	Subscriber Arbitrary File Upload in Restaurant Zone <= 0.7.8 versions.	9.9	More Details
CVE-2026-39589	Subscriber Arbitrary File Upload in Webenvo <= 0.0.6 versions.	9.9	More Details

CVE-2026-35268	Vulnerability in the Identity Manager product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via T3, IIOP to compromise Identity Manager. While the vulnerability is in Identity Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Identity Manager. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2026-46918	Vulnerability in the Oracle Process Manufacturing Product Development product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Process Manufacturing Product Development. While the vulnerability is in Oracle Process Manufacturing Product Development, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Process Manufacturing Product Development. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2026-27041	Contributor Arbitrary File Upload in Unlimited Elements for Elementor (Premium) <= 2.0.6 versions.	9.9	More Details
CVE-2026-25446	Subscriber Arbitrary File Upload in WishList Member X <= 3.29.0 versions.	9.9	More Details
CVE-2026-22327	Subscriber Arbitrary File Upload in Restaurt <= 1.0.4 versions.	9.9	More Details
CVE-2025-60218	Subscriber Arbitrary File Upload in PT Luxa Addons <= 1.2.2 versions.	9.9	More Details
CVE-2024-52488	Subscriber Arbitrary File Upload in Grip <= 1.0.9 versions.	9.9	More Details
CVE-2026-46964	Vulnerability in the Oracle Universal Work Queue product of Oracle E-Business Suite (component: Work Provider Site Level Administration). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Universal Work Queue. While the vulnerability is in Oracle Universal Work Queue, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Universal Work Queue. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2026-56142	In JetBrains Hub before 2026.1.13757, 2025.3.148033, 2025.2.148048, 2025.1.148120, 2024.3.148430, 2024.2.148429 privilege escalation by attaching authentication details to accounts was possible	9.9	More Details
CVE-2026-46933	Vulnerability in the Oracle Applications Manager product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Applications Manager. While the vulnerability is in Oracle Applications Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Applications Manager. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2026-46963	Vulnerability in the Oracle Universal Work Queue product of Oracle E-Business Suite (component: Work Provider Site Level Administration). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Universal Work Queue. While the vulnerability is in Oracle Universal Work Queue, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Universal Work Queue. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2026-48584	Execution with unnecessary privileges in Azure Synapse allows an authorized attacker to elevate privileges over a network.	9.9	More Details

CVE-2026-35313	Vulnerability in the Oracle Access Manager product of Oracle Fusion Middleware (component: Authentication Engine). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Access Manager. While the vulnerability is in Oracle Access Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Access Manager. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2026-35316	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Content. While the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Content. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2026-46765	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Composer). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Portal. While the vulnerability is in Oracle WebCenter Portal, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Portal. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2026-35294	Vulnerability in the Identity Manager Connector product of Oracle Fusion Middleware (component: Mainframe Connectors). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Identity Manager Connector. While the vulnerability is in Identity Manager Connector, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Identity Manager Connector. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2026-35284	Vulnerability in the Oracle WebCenter Enterprise Capture product of Oracle Fusion Middleware (component: Client Bundle). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via T3, IIOP to compromise Oracle WebCenter Enterprise Capture. While the vulnerability is in Oracle WebCenter Enterprise Capture, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Enterprise Capture. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2026-35323	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Content. While the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Content. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2026-46782	Vulnerability in the Oracle WebCenter Enterprise Capture product of Oracle Fusion Middleware (component: Client Bundle). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Enterprise Capture. While the vulnerability is in Oracle WebCenter Enterprise Capture, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Enterprise Capture. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware		

CVE-2026-35321	(component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Content. While the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Content. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2026-46767	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Composer). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Portal. While the vulnerability is in Oracle WebCenter Portal, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Portal. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2026-55255	Langflow is a tool for building and deploying AI-powered agents and workflows. Prior to 1.9.2, an Insecure Direct Object Reference (IDOR) vulnerability in /api/v1/responses endpoint allows an authenticated attacker to execute any flow belonging to another user by specifying the victim's flow ID in the request. This vulnerability is fixed in 1.9.2.	9.9	More Details
CVE-2026-56274	Flowise before 3.1.2 contains multiple OS command injection vulnerabilities in the Custom MCP Server feature due to incomplete command-flag validation and a regex bypass in local file access restrictions. An attacker with a Flowise account of any role, or API access with view/update permissions for chatflows, can configure a malicious MCP server to bypass the validateCommandFlags blocklist (for example, 'docker build' is not blocked, and 'npx --yes' is not blocked while only '-y' is) and the validateArgsForLocalFileAccess checks, resulting in execution of arbitrary commands on the Flowise host.	9.9	More Details
CVE-2026-35283	Vulnerability in the Oracle WebCenter Enterprise Capture product of Oracle Fusion Middleware (component: Client Bundle). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via T3, IIOP to compromise Oracle WebCenter Enterprise Capture. While the vulnerability is in Oracle WebCenter Enterprise Capture, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Enterprise Capture. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2026-35285	Vulnerability in the Oracle WebCenter Enterprise Capture product of Oracle Fusion Middleware (component: Client Bundle). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via T3, IIOP to compromise Oracle WebCenter Enterprise Capture. While the vulnerability is in Oracle WebCenter Enterprise Capture, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Enterprise Capture. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2026-46792	Vulnerability in the Identity Manager Connector product of Oracle Fusion Middleware (component: Generic Unix Connector). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Identity Manager Connector. While the vulnerability is in Identity Manager Connector, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Identity Manager Connector. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2026-46793	Vulnerability in the Identity Manager Connector product of Oracle Fusion Middleware (component: Database User). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Identity Manager Connector. While the vulnerability is in Identity Manager Connector, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Identity Manager Connector. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details

CVE-2026-46794	Vulnerability in the Identity Manager Connector product of Oracle Fusion Middleware (component: Generic Unix Connector). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via SSH to compromise Identity Manager Connector. While the vulnerability is in Identity Manager Connector, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Identity Manager Connector. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2026-35282	Vulnerability in the Oracle WebCenter Enterprise Capture product of Oracle Fusion Middleware (component: Client Bundle). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via T3, IIOP to compromise Oracle WebCenter Enterprise Capture. While the vulnerability is in Oracle WebCenter Enterprise Capture, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Enterprise Capture. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2026-35281	Vulnerability in the Oracle WebCenter Enterprise Capture product of Oracle Fusion Middleware (component: Client Bundle). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via T3, IIOP to compromise Oracle WebCenter Enterprise Capture. While the vulnerability is in Oracle WebCenter Enterprise Capture, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Enterprise Capture. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2026-35280	Vulnerability in the Oracle WebCenter Enterprise Capture product of Oracle Fusion Middleware (component: Client Bundle). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via T3, IIOP to compromise Oracle WebCenter Enterprise Capture. While the vulnerability is in Oracle WebCenter Enterprise Capture, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Enterprise Capture. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2026-46779	Vulnerability in the Oracle WebCenter Enterprise Capture product of Oracle Fusion Middleware (component: Client Bundle). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via T3 to compromise Oracle WebCenter Enterprise Capture. While the vulnerability is in Oracle WebCenter Enterprise Capture, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Enterprise Capture. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2026-46802	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Security Framework). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Portal. While the vulnerability is in Oracle WebCenter Portal, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Portal. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2026-35286	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Content. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2026-42380	Unauthenticated PHP Object Injection in AI Lab < 5.4.2 versions.	9.8	More Details

CVE-2026-35278	Vulnerability in the PeopleSoft Enterprise PT PeopleTools product of Oracle PeopleSoft (component: Performance Monitor). Supported versions that are affected are 8.61 and 8.62. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PT PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PT PeopleTools. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2026-35310	Vulnerability in the Oracle Coherence product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0 and 15.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Coherence. Successful attacks of this vulnerability can result in takeover of Oracle Coherence. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2026-35296	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Sites. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2026-40725	Unauthenticated PHP Object Injection in WooCommerce Product Filters < 2.0.6 versions.	9.8	More Details
CVE-2026-35293	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Sites. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2026-39529	Unauthenticated PHP Object Injection in Elementra <= 1.0.9 versions.	9.8	More Details
CVE-2026-53753	Crawl4AI is an open-source LLM friendly web crawler & scraper. Prior to 0.8.7, the _safe_eval_expression() function in the computed fields feature uses an AST validator that only blocks attributes starting with underscore. Python generator and frame object attributes (gi_frame, f_back, f_builtins) do NOT start with underscore, enabling a complete sandbox escape to achieve arbitrary code execution. The attack requires no authentication (JWT disabled by default) and is triggered via POST /crawl with a crafted extraction schema. This vulnerability is fixed in 0.8.7.	9.8	More Details
CVE-2026-32966	DataSource API Missing Authorization Check Leads to Arbitrary Data Source Metadata Disclosure in Apache DolphinScheduler. This issue affects Apache DolphinScheduler: before 3.4.2. Users are recommended to upgrade to version 3.4.2, which fixes the issue.	9.8	More Details
CVE-2026-27429	Unauthenticated PHP Object Injection in Nifty <= 1.4.1 versions.	9.8	More Details
CVE-2026-27395	Unauthenticated Privilege Escalation in Support Board < 3.8.9 versions.	9.8	More Details
CVE-2026-35300	Vulnerability in the WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0 and 15.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via TCP to compromise WebLogic Server. Successful attacks of this vulnerability can result in takeover of WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2026-35304	Vulnerability in the Oracle Coherence product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0 and 15.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Coherence. Successful attacks of this vulnerability can result in takeover of Oracle Coherence. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details

CVE-2026-54130	Missing authentication for critical function in M365 Copilot allows an unauthorized attacker to disclose information over a network.	9.8	More Details
CVE-2026-40624	Improper input validation in AVer PTC500S, PTC115, PTC500+, and PTC115+ cameras may allow a remote, unauthenticated attacker to achieve arbitrary code execution via a specially crafted web request.	9.8	More Details
CVE-2026-47846	Bitnami Cassandra container images are affected by a retained default superuser vulnerability. When a custom administrator account is configured via the CASSANDRA_USER environment variable, the container initialization script creates the new superuser account but fails to drop the built-in cassandra account in certain scenarios. This leaves the default cassandra:cassandra superuser active as an unintended access path. Affected versions — Container image: 4.0.x prior to 4.0.20-photon-5-r7; 4.1.x prior to 4.1.11-photon-5-r7; 5.0.x prior to 5.0.8-photon-5-r4 / 5.0.8-debian-12-r3.	9.8	More Details
CVE-2026-54390	JTL Shop versions 5.2.0 through 5.7.1 contains a server-side template injection vulnerability that allows unauthenticated attackers to inject malicious template syntax due to unsanitized user-supplied input passed to the Smarty template engine. Attackers can exploit this flaw to read sensitive server-side values such as database credentials and encryption keys, and on versions 5.4.0 through 5.7.1, leverage registered Smarty modifiers including unserialize and file_get_contents to write a webshell to the web root and execute arbitrary commands as the web server user.	9.8	More Details
CVE-2026-49058	Unauthenticated Privilege Escalation in LoginPress Pro <= 6.2.2 versions.	9.8	More Details
CVE-2026-49075	Contributor PHP Object Injection in JetEngine <= 3.8.9.1 versions.	9.8	More Details
CVE-2025-71323	picklescan before 0.0.33 fails to block the ctypes module, allowing attackers to achieve remote code execution by invoking direct syscalls and accessing raw memory. Attackers can craft malicious pickle files using ctypes.WinDLL to load kernel32.dll and execute arbitrary commands, bypassing sandbox protections and gadget chain detection.	9.8	More Details
CVE-2026-47103	Python StateMachine versions 3.0.0 before 3.2.0 contains a remote code execution vulnerability that allows attackers to execute arbitrary code by supplying malicious SCXML documents containing crafted `<data expr="...">` attributes evaluated unsafely. The SCXMLProcessor passes attacker-controlled expression strings through a call chain ending in Python's built-in eval() without sandboxing, enabling arbitrary code execution in the context of the hosting process.	9.8	More Details
CVE-2025-71325	picklescan before 0.0.27 contains a parsing logic error in the _list_globals function when handling STACK_GLOBAL opcodes, failing to track arguments in the correct range and allowing malicious pickle files to bypass detection. Attackers can craft pickle files with arguments at position zero to trigger unexpected exceptions and evade security scanning.	9.8	More Details
CVE-2026-53873	picklescan before 1.0.4 contains an incomplete blocklist for the profile module that fails to block the module-level profile.run() function, allowing attackers to achieve arbitrary code execution via exec(). Attackers can craft malicious pickle files calling profile.run(statement) to execute arbitrary Python code while picklescan reports zero security issues.	9.8	More Details
CVE-2026-53874	picklescan before 1.0.1 contains an unsafe deserialization vulnerability allowing unauthenticated users to execute arbitrary code by hiding eval calls nested under callable objects via getattr. Attackers can embed malicious code in pickle files that evades detection but executes when the pickle is loaded from untrusted sources.	9.8	More Details
CVE-2026-53805	NVIDIA Spatial Intelligence Lab's (SIL) GEN3C contains an unauthenticated remote code execution vulnerability in the inference API server where the /request-inference and /seed-model endpoints deserialize raw HTTP request bodies using Python's pickle.loads() without authentication or input validation. Attackers can supply a crafted payload containing a __reduce__ gadget to the inference API port to achieve remote code execution as the inference process.	9.8	More Details
CVE-2026-49108	Unauthenticated PHP Object Injection in Moderno < 1.43 versions.	9.8	More Details

CVE-2025-69127	Unauthenticated PHP Object Injection in Plumbing <= 1.6 versions.	9.8	More Details
CVE-2025-69111	Unauthenticated PHP Object Injection in Reisen <= 1.4.1 versions.	9.8	More Details
CVE-2025-60236	Deserialization of Untrusted Data vulnerability in EMV Creatify allows Object Injection. This issue affects Creatify: from n/a through 1.5.	9.8	More Details
CVE-2025-60231	Deserialization of Untrusted Data vulnerability in EMV The Hospital nrghospital allows Object Injection. This issue affects The Hospital: from n/a through 1.8.1.	9.8	More Details
CVE-2025-60230	Deserialization of Untrusted Data vulnerability in Themeton The Barber Shop allows Object Injection. This issue affects The Barber Shop: from n/a through 1.9.	9.8	More Details
CVE-2025-60229	Deserialization of Untrusted Data vulnerability in Themeton Lagom allows Object Injection. This issue affects Lagom: from n/a through 2.0.	9.8	More Details
CVE-2026-55740	Nur-Alam39 bus-ticket (no released versions; latest commit 459cabdbeb99c00225b26e46e3c2c30ae1de7bad) contains an unauthenticated SQL injection vulnerability in bus_info.php. The busid parameter received via HTTP POST is concatenated directly into a MySQL query (select * from bus_info where id=$busid) without sanitization, escaping, or parameterization, and in a numeric (unquoted) context. A remote, unauthenticated attacker can inject arbitrary SQL — for example a UNION-based payload such as busid=-1 UNION SELECT 1,2,3,4,5,6 — to read arbitrary data from the bus_service database. The application connects to the database as the MySQL root account with an empty password, increasing the potential impact. The query is executed via mysqli_query(), which does not permit stacked (semicolon-separated) statements.	9.8	More Details
CVE-2026-54807	Unauthenticated Privilege Escalation in Registration Form for WooCommerce <= 1.0.9 versions.	9.8	More Details
CVE-2026-54806	Unauthenticated PHP Object Injection in WP Activity Log <= 5.6.3.1 versions.	9.8	More Details
CVE-2026-54803	Subscriber Privilege Escalation in SMS Alert Order Notifications <= 3.9.4 versions.	9.8	More Details
CVE-2026-54194	Contributor PHP Object Injection in Fusion Builder <= 3.15.4 versions.	9.8	More Details
CVE-2026-54419	claudiopizzillo PIAF-HMS (PBX-In-A-Flash Hotel Management System; no released versions, latest commit 389d2633441b65ced1c104212cd62be2bfca21e5) contains multiple unauthenticated SQL injection vulnerabilities. The application has no authentication mechanism and passes user-supplied HTTP parameters directly into deprecated mysql_query() calls via string concatenation, without sanitization, escaping, or parameterization. Affected sinks include rooms.php (DELETE FROM Rooms WHERE ID = $_GET['ID'], unquoted numeric context), checkuser.php (WHERE Ext = '$_GET["Ext"]'), ec.php (date/extension parameters in a WHERE), checkin.php and wakeup.php ($_POST values into INSERT statements), bills.php ($_POST fields built into a WHERE clause), and rates.php and checkout.php. A remote, unauthenticated attacker can inject arbitrary SQL to read, modify, or delete arbitrary records in the backing database (e.g. rooms.php?ID=1 OR 1=1 deletes all room records). Note: queries run via the legacy mysql_* extension, which does not permit stacked statements.	9.8	More Details
CVE-2026-8024	A remote, unauthenticated attacker may exploit a deserialization of untrusted data vulnerability in ibaPDA or ibaDatCoordinator to gain full access to the affected systems.	9.8	More Details
CVE-2026-52706	Unauthenticated PHP Object Injection in JetEngine <= 3.8.10 versions.	9.8	More Details
CVE-2026-38714	InHand Networks IR912 V1.0.0.r20042 and IR915 V1.0.0.r20042 (including earlier versions) were discovered to contain a command injection vulnerability in the Python configuration function. This vulnerability allows remote attackers to execute arbitrary commands as root via a crafted input.	9.8	More Details
	InHand Networks IR912 V1.0.0.r20042 and IR915 V1.0.0.r20042 (including earlier versions)		

CVE-2026-38715	were discovered to contain a command injection vulnerability in the log viewing function. This vulnerability allows remote attackers to execute arbitrary commands as root via a crafted input.	9.8	More Details
CVE-2026-49767	Unauthenticated Broken Authentication in wpForo Forum <= 3.1.0 versions.	9.8	More Details
CVE-2026-49107	Unauthenticated PHP Object Injection in Thrive Apprentice < 10.8.10.2 versions.	9.8	More Details
CVE-2026-38716	InHand Networks IR912 V1.0.0.r20042 and IR915 V1.0.0.r20042 (including earlier versions) were discovered to contain a command injection vulnerability in the Python application export function. This vulnerability allows remote attackers to execute arbitrary commands as root via a crafted input.	9.8	More Details
CVE-2026-38717	InHand Networks IR912 V1.0.0.r20042 and IR915 V1.0.0.r20042 (including earlier versions) were discovered to contain a command injection vulnerability in the file upload function. The vulnerability allows remote attackers to execute arbitrary commands as root via a crafted input.	9.8	More Details
CVE-2026-54103	The U.S. Government Accountability Office (GAO) Electronic Protest Docketing System (EPDS) and Civilian Board of Contract Appeals (CBCA) Electronic Docketing System (EDS) does not authenticate password change requests to the '/update-profile/N' API endpoint. A remote, unauthenticated attacker could change an arbitrary user's password.	9.8	More Details
CVE-2026-7515	The BetterDocs Pro plugin for WordPress is vulnerable to Local File Inclusion in versions up to, and including, 3.8.0 via the `doc_style` parameter. This makes it possible for unauthenticated attackers to include and execute arbitrary .php files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where .php file types can be uploaded and included.	9.8	More Details
CVE-2026-54414	FileRise before 3.16.0 is vulnerable to path traversal in the shared-folder upload endpoint (/api/folder/uploadToSharedFolder.php), leading to arbitrary file write and administrator account takeover. The upload filename is validated by FolderController with basename() and REGEX_FILE_NAME, which permit URL-encoded sequences (the regex blocks / and \ but not %). The raw filename is then passed to UploadModel::handleUpload, where it is reconstructed as trim(urldecode(basename($fileName))), re-introducing path separators after validation (e.g. ..%2fusers%2fusers.txt becomes ../users/users.txt). UploadNamePolicy::isAllowedForWrite() applies basename() internally and therefore only evaluates the final component (users.txt), allowing the traversal sequence to pass the extension policy. The destination path is then used directly in move_uploaded_file() with no realpath containment check, allowing a write outside the intended upload directory. An attacker who possesses a valid, non-expired, upload-enabled shared-folder link/token (which are designed to be shared publicly) can overwrite users/users.txt to create an administrator account, resulting in unauthenticated admin takeover and, depending on configuration, remote code execution. Exploitation requires possession of a valid, non-expired, upload-enabled shared-folder link/token. This issue is fixed in 3.16.0, which URL-decodes before validation and rejects any path separators in the upload filename.	9.8	More Details
CVE-2025-71321	picklescan before 0.0.33 contains an arbitrary file writing vulnerability that allows attackers to bypass the dangerous blocklist by using distutils.file_util.write_file. Attackers can construct malicious pickle objects to overwrite critical system files and achieve denial of service or remote code execution.	9.8	More Details
CVE-2026-10094	A Path Traversal vulnerability affecting SOLIDWORKS Visualize from SOLIDWORKS Desktop Release 2024 through SOLIDWORKS Desktop Release 2026 could allow an attacker to write arbitrary files on the server.	9.8	More Details
CVE-2022-50972	WooCommerce 7.1.0 contains a remote code execution vulnerability that allows attackers to execute arbitrary PHP code by injecting shell commands through the product-type parameter. Attackers can send requests to the class-wc-meta-box-product-images.php endpoint with unsanitized product-type values to write malicious PHP files to the web root.	9.8	More Details
	Vulnerability in the Siebel Apps - Marketing product of Oracle Siebel CRM (component: Marketing). Supported versions that are affected are 17.0-26.5. Easily exploitable vulnerability		

CVE-2026-46890	allows unauthenticated attacker with network access via HTTP to compromise Siebel Apps - Marketing. Successful attacks of this vulnerability can result in takeover of Siebel Apps - Marketing. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2026-46889	Vulnerability in the Siebel Apps - Marketing product of Oracle Siebel CRM (component: Marketing). Supported versions that are affected are 17.0-26.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel Apps - Marketing. Successful attacks of this vulnerability can result in takeover of Siebel Apps - Marketing. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2026-46887	Vulnerability in the Siebel Apps - Marketing product of Oracle Siebel CRM (component: Marketing). Supported versions that are affected are 17.0-26.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel Apps - Marketing. Successful attacks of this vulnerability can result in takeover of Siebel Apps - Marketing. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2026-46884	Vulnerability in the Siebel Apps - Marketing product of Oracle Siebel CRM (component: Marketing). Supported versions that are affected are 17.0-26.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel Apps - Marketing. Successful attacks of this vulnerability can result in takeover of Siebel Apps - Marketing. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2026-46883	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Enterprise Infrastructure Security). Supported versions that are affected are 9.2.0.0-9.2.26.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via JDENET to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in takeover of JD Edwards EnterpriseOne Tools. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2026-46882	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Enterprise Infrastructure Security). Supported versions that are affected are 9.2.0.0-9.2.26.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via JDENET to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in takeover of JD Edwards EnterpriseOne Tools. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2026-46881	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Enterprise Infrastructure Security). Supported versions that are affected are 9.2.0.0-9.2.26.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via JDENET to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in takeover of JD Edwards EnterpriseOne Tools. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2026-46880	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Enterprise Infrastructure Security). Supported versions that are affected are 9.2.0.0-9.2.26.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via JDENET to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in takeover of JD Edwards EnterpriseOne Tools. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2026-46879	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Enterprise Infrastructure Security). Supported versions that are affected are 9.2.0.0-9.2.26.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via JDENET to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in takeover of JD Edwards EnterpriseOne Tools. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details

CVE-2026-46878	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Enterprise Infrastructure Security). Supported versions that are affected are 9.2.0.0-9.2.26.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via JDENET to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in takeover of JD Edwards EnterpriseOne Tools. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2019-25763	WordPress Ultimate Addons for Beaver Builder 1.2.4.1 contains an authentication bypass vulnerability that allows attackers to gain unauthorized access by exploiting the social media login form functionality. Attackers can submit a POST request to the admin-ajax.php endpoint with the uabb-lf-google-submit action, a valid administrator email address, and a valid nonce to obtain session cookies and authenticate as that user.	9.8	More Details
CVE-2024-58351	Flowise before 2.1.4 allows configuration to be injected into the Chainflow during execution via the overrideConfig option, supported in both the frontend web integration and the backend Prediction API. Because this feature is enabled by default with no allow-list of permitted variables and relies on vm2 for sandboxing, an attacker can abuse it to achieve remote code execution and sandbox escape, denial of service by crashing the server, server-side request forgery, prompt injection, and server variable and data exfiltration. These issues are self-targeted and do not persist to other users.	9.8	More Details
CVE-2026-46783	Vulnerability in the WebCenter Content: Imaging product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise WebCenter Content: Imaging. Successful attacks of this vulnerability can result in takeover of WebCenter Content: Imaging. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2026-46860	Vulnerability in the MySQL Router product of Oracle MySQL (component: Router: General). Supported versions that are affected are 9.0.0-9.7.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise MySQL Router. Successful attacks of this vulnerability can result in takeover of MySQL Router. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2026-46859	Vulnerability in the Oracle Agile PLM product of Oracle Supply Chain (component: Security). The supported version that is affected is 9.3.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Agile PLM. Successful attacks of this vulnerability can result in takeover of Oracle Agile PLM. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2026-56265	Crawl4AI before 0.8.7 contains an authentication bypass vulnerability due to a hardcoded default JWT signing key in the Docker API server. Attackers who know the default key can forge valid authentication tokens for any user, bypassing authentication and gaining full access to protected functionality.	9.8	More Details
CVE-2026-46857	Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Oracle Management Service). Supported versions that are affected are 13.5 and 24.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Enterprise Manager Base Platform. Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Manager Base Platform. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2026-12866	All versions of the package expr-eval are vulnerable to Code Execution via the toJSFunction() API. An attacker can execute arbitrary JavaScript by supplying crafted expressions that are compiled into native code using new Function(). Because user-controlled expressions are transformed directly into executable JavaScript, attackers can escape the intended expression sandbox and run arbitrary code within the application's context.	9.8	More Details
	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Security Framework). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network		

CVE-2026-46845	access via HTTPS to compromise Oracle WebCenter Portal. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Portal. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2026-7664	IBM Langflow OSS 1.0.0 through 1.8.4 could allow unauthenticated attackers to access protected MCP project resources and execute MCP operations due to improper authorization enforcement in the Streamable MCP transport endpoint.	9.8	More Details
CVE-2026-46797	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Sites. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2026-46799	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Sites. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2026-46801	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Sites. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2026-46813	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Content. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2026-56315	picklescan before 1.0.4 fails to block at least seven Python standard library modules (including uuid, _osx_support, _aix_support, _pyrepl.pager, and imaplib) exposing eight functions that provide direct arbitrary command execution. Attackers can craft malicious pickle files importing these unblocked modules to achieve remote code execution while bypassing picklescan's safety validation entirely.	9.8	More Details
CVE-2026-11551	The Branda plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 3.4.29. This is due to the plugin not properly validating a user's identity prior to updating their password. This makes it possible for unauthenticated attackers to change arbitrary user's passwords, including administrators, and leverage that to gain access to their account.	9.8	More Details
CVE-2025-71320	picklescan before 0.0.33 contains an incomplete deny-list that fails to block pydoc.locate and operator.methodcaller functions, allowing attackers to bypass security checks. Remote attackers can craft malicious pickle files using these unblocked functions to achieve arbitrary code execution when the pickle is deserialized.	9.8	More Details
CVE-2026-46807	Vulnerability in the Identity Manager product of Oracle Fusion Middleware (component: OIM Legacy UI). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Identity Manager. Successful attacks of this vulnerability can result in takeover of Identity Manager. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2025-60205	Unauthenticated PHP Object Injection in ThemeREX Addons <= 2.36.1.1 versions.	9.8	More Details

CVE-2026-35312	Vulnerability in the Oracle Virtual Directory product of Oracle Fusion Middleware (component: Virtual Directory Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via LDAP to compromise Oracle Virtual Directory. Successful attacks of this vulnerability can result in takeover of Oracle Virtual Directory. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2026-35319	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Content. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2026-56141	In JetBrains Hub before 2026.1.13757, 2025.3.148033, 2025.2.148048, 2025.1.148120, 2024.3.148430, 2024.2.148429 account takeover via predictable restore codes was possible	9.8	More Details
CVE-2026-51843	Tenda AC7 v15.03.06.44 contains a stack buffer overflow vulnerability in the /goform/AdvSetMacMtuWan interface via the wanMTU parameter.	9.8	More Details
CVE-2025-69122	Unauthenticated PHP Object Injection in SeaFood Company <= 1.4 versions.	9.8	More Details
CVE-2026-51844	Tenda AC7 v15.03.06.44 contains a stack buffer overflow vulnerability in the /goform/AdvSetMacMtuWan interface via the cloneType parameter.	9.8	More Details
CVE-2026-46919	Vulnerability in the Siebel CRM Cloud Applications product of Oracle Siebel CRM (component: Siebel Cloud Manager). Supported versions that are affected are 17.0-26.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel CRM Cloud Applications. Successful attacks of this vulnerability can result in takeover of Siebel CRM Cloud Applications. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2026-51845	Tenda AC7 v15.03.06.44 contains a stack buffer overflow vulnerability in the /goform/AdvSetMacMtuWan interface via the mac parameter.	9.8	More Details
CVE-2026-51846	In Tenda AC7 v15.03.06.44, the wanSpeed parameter of the route /goform/AdvSetMacMtuWan has a stack buffer overflow vulnerability that can lead to remote arbitrary code execution.	9.8	More Details
CVE-2026-46766	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Content. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2026-48773	ProxySQL is a proxy for MySQL and its forks, as well as PostgreSQL. Versions 2.0.18 through 3.0.8 have a pre-authentication heap memory corruption vulnerability in the MySQL and PostgreSQL protocol first-read paths. A remote unauthenticated client can declare an oversized first packet length, and ProxySQL passes that attacker-controlled length directly to `recv()` while writing into a fixed 32 KB input queue. Version 3.0.9 patches the issue.	9.8	More Details
CVE-2026-46909	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Enterprise Infrastructure Security). Supported versions that are affected are 9.2.0.0-9.2.26.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in takeover of JD Edwards EnterpriseOne Tools. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2026-46773	Vulnerability in the Oracle Unified Directory product of Oracle Fusion Middleware (component: OUD Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via LDAP to compromise Oracle Unified Directory. Successful attacks of this vulnerability can result in	9.8	More Details

	takeover of Oracle Unified Directory. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).		
CVE-2026-46774	Vulnerability in the Oracle Unified Directory product of Oracle Fusion Middleware (component: OUD Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via RMI to compromise Oracle Unified Directory. Successful attacks of this vulnerability can result in takeover of Oracle Unified Directory. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2026-46905	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Web Runtime Security). Supported versions that are affected are 9.2.0.0-9.2.26.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in takeover of JD Edwards EnterpriseOne Tools. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2026-46904	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Enterprise Infrastructure Security). Supported versions that are affected are 9.2.0.0-9.2.26.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via JDENET to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in takeover of JD Edwards EnterpriseOne Tools. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2026-46902	Vulnerability in the Oracle Enterprise Command Center Framework product of Oracle E-Business Suite (component: Core). Supported versions that are affected are V15 and V16. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Enterprise Command Center Framework. Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Command Center Framework. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2026-35309	Vulnerability in the Oracle Coherence product of Oracle Fusion Middleware (component: Centralized Third Party Jars). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0 and 15.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Coherence. Successful attacks of this vulnerability can result in takeover of Oracle Coherence. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2025-69179	Unauthenticated Privilege Escalation in Support Ticket Management System <= 1.9 versions.	9.8	More Details
CVE-2025-69108	Unauthenticated PHP Object Injection in Hot Coffee <= 1.7 versions.	9.8	More Details
CVE-2026-11807	A missing authorization vulnerability was found in the Event-Driven Ansible (EDA) websocket API. The /api/eda/ws/ansible-rulebook endpoint does not verify user permissions when processing Worker messages. Any authenticated user can send a forged message with an arbitrary activation_id to receive plaintext credentials associated with that activation, including OAuth tokens, vault passwords, and SSH keys.	9.6	More Details
CVE-2026-53662	immich is a high performance self-hosted photo and video management solution. From commit 4ffa26c9 until 4eb1003, a reflected cross-site scripting (XSS) vulnerability on the /auth/login page allows an attacker to fully compromise any authenticated user's account with a single link click. The continue query parameter is read from the URL and passed to SvelteKit's redirect() without any scheme or origin validation, allowing attacker-controlled JavaScript to execute inside Immich's origin. The payload then uses the victim's existing session to mint an all-permission API key on their account, leading to persistent account takeover. This vulnerability is fixed in commit 4eb1003.	9.6	More Details
	Cotonti 1.0.0 (master branch, commit f43f1fc3) is vulnerable to Cross-Site Request Forgery in the administration rights handler. In system/admin/admin.rights.php, the rights update action ('a=update') modifies group access rights (including via cot_auth_add_group) without calling		

CVE-2026-55742	cot_check_xg() to validate the anti-CSRF token. A remote attacker who lures an authenticated administrator into visiting a malicious page can force the browser to submit a forged request that grants elevated permissions to an attacker-controlled group, escalating privileges to administrator. Because Cotonti administrators can modify templates and configuration, this can be further leveraged toward remote code execution.	9.6	More Details
CVE-2026-10789	A maliciously crafted webpage, when visited by a user with Autodesk Fusion Desktop running and the MCP extension enabled, can trigger a vulnerability in the MCP extension that could allow arbitrary code execution. A successful exploit may allow code to execute with the privileges of the current user.	9.6	More Details
CVE-2026-56397	SiYuan before v3.6.1 fails to sanitize package metadata and README content in the Bazaar marketplace, allowing malicious package authors to inject arbitrary HTML and JavaScript. Attackers can achieve remote code execution on any user browsing the Bazaar by embedding XSS payloads in package displayName, description, or README fields, exploiting Electron's nodeIntegration setting to execute OS commands.	9.6	More Details
CVE-2026-56395	SiYuan before v3.6.1 fails to sanitize package metadata and README content in the Bazaar marketplace, allowing malicious package authors to inject arbitrary HTML and JavaScript. Attackers can achieve remote code execution on any user browsing the Bazaar by embedding XSS payloads in package displayName, description, or README fields, exploiting Electron's nodeIntegration setting to execute OS commands.	9.6	More Details
CVE-2026-48582	Missing authorization in Microsoft Exchange Online allows an authorized attacker to elevate privileges over a network.	9.6	More Details
CVE-2026-48519	Langflow is a tool for building and deploying AI-powered agents and workflows. Prior to 1.9.2, the "Shareable Playground" (or "Public Flows" in code) contains a critical RCE vulnerability. Shareable Playground feature works by enabling the execution of workflows by unauthenticated users, by accessing a link. Specifically, it enables the route /api/v1/build_public_tmp to execute any public flow, given a public flow ID. When the route executes the flow, it allows for providing arbitrary custom Python code as the nodes code, inside the JSON payload. The vulnerable field is data.nodes[X].data.node.template.code.value. This vulnerability is fixed in 1.9.2.	9.6	More Details
CVE-2026-55447	Langflow is a tool for building and deploying AI-powered agents and workflows. Prior to 1.9.2, by controlling a files that are digested into the RAG, an attacker can direct the node to read any file on the file-system by absolute path. All components based on BaseFileComponent are vulnerable to the vulnerability. This includes Docling (DoclingInlineComponent), Docling Serve, DoclingRemoteComponent), Read File (FileComponent), NVIDIA Retriever Extraction (NvidiaIngestComponent), Video File (VideoFileComponent), and Unstructured API (UnstructuredComponent). This vulnerability is fixed in 1.9.2.	9.6	More Details
CVE-2026-28381	The Snowflake datasource allows for GET/PUT commands, which can allow any user with access to run queries against the data source to read/write files between the local grafana server and the connected Snowflake host.	9.6	More Details
CVE-2026-54588	Poweradmin is a web-based DNS administration tool for PowerDNS server. Versions prior to 4.2.4 and 4.3.3 use the attacker-controlled `HTTP_HOST` request header as the authoritative source for building callback URLs in its OIDC, SAML, and logout authentication flows without any validation. An unauthenticated attacker can poison the `redirect_uri` sent to the Identity Provider, causing the IdP to redirect the victim's authorization code to an attacker-controlled server - resulting in full account takeover with no credentials required. Versions 4.2.4 and 4.3.3 patch the issue.	9.6	More Details
CVE-2026-55743	The shell tool command allowlist in the SecurityPolicy of OpenHuman desktop agent through 0.54.0 (default Supervised security policy) can be bypassed to execute arbitrary OS commands with the privileges of the desktop user. Two flaws in src/openhuman/security/policy.rs combine: (1) is_args_safe() blocks the find flags -exec and -ok but not the functionally identical -execdir and -okdir, which also execute an arbitrary command for each matched file; and (2) skip_env_assignments() strips leading inline KEY=value environment-variable assignments before allowlist validation, so a command such as GIT_EXTERNAL_DIFF=<cmd> git diff is validated as the allowed git diff but, when executed via the shell, runs <cmd> through git's environment-driven hooks (for example GIT_EXTERNAL_DIFF or GIT_SSH_COMMAND). Because the sandbox is the primary trust	9.6	More Details

	boundary between untrusted LLM-processed content and the host operating system, an attacker can achieve remote code execution via indirect prompt injection: a malicious document, email, calendar event, or web page ingested by the agent instructs it to run a benign-looking allowlisted command, resulting in arbitrary command execution, data exfiltration, arbitrary file read/write, and lateral movement on the user's machine. The issue was fixed in commit 60050aa09a870f53ed7e4cd40ed41fd2860329e7 (first released in 0.54.22-staging; first stable release 0.56.0), which blocks -execdir/-okdir for find.		
CVE-2026-46911	Vulnerability in the JD Edwards EnterpriseOne Project Costing product of Oracle JD Edwards (component: Job Costing). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via JDENET to compromise JD Edwards EnterpriseOne Project Costing. While the vulnerability is in JD Edwards EnterpriseOne Project Costing, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all JD Edwards EnterpriseOne Project Costing accessible data as well as unauthorized access to critical data or complete access to all JD Edwards EnterpriseOne Project Costing accessible data. CVSS 3.1 Base Score 9.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N).	9.6	More Details
CVE-2026-46853	Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Metadata Plugin). Supported versions that are affected are 13.5 and 24.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Enterprise Manager Base Platform. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Enterprise Manager Base Platform, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Manager Base Platform. CVSS 3.1 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).	9.6	More Details
CVE-2026-46861	Vulnerability in the MySQL NDB Cluster product of Oracle MySQL (component: Cluster: NDB Operator). Supported versions that are affected are 8.0.11-8.0.46, 8.4.0-8.4.9 and 9.0.0-9.7.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise MySQL NDB Cluster. While the vulnerability is in MySQL NDB Cluster, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL NDB Cluster accessible data as well as unauthorized access to critical data or complete access to all MySQL NDB Cluster accessible data. CVSS 3.1 Base Score 9.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N).	9.6	More Details
CVE-2026-12440	Use after free in DigitalCredentials in Google Chrome on Windows prior to 149.0.7827.155 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	9.6	More Details
CVE-2026-46789	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Content. CVSS 3.1 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).	9.6	More Details
CVE-2026-46786	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Content. CVSS 3.1 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).	9.6	More Details

CVE-2026-46856	Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Metadata Plugin). Supported versions that are affected are 13.5 and 24.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Enterprise Manager Base Platform. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Enterprise Manager Base Platform, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Manager Base Platform. CVSS 3.1 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).	9.6	More Details
CVE-2026-46899	Vulnerability in the Oracle Enterprise Command Center Framework product of Oracle E-Business Suite (component: Core). Supported versions that are affected are V15 and V16. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Enterprise Command Center Framework. While the vulnerability is in Oracle Enterprise Command Center Framework, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Enterprise Command Center Framework accessible data as well as unauthorized access to critical data or complete access to all Oracle Enterprise Command Center Framework accessible data. CVSS 3.1 Base Score 9.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N).	9.6	More Details
CVE-2026-46906	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Enterprise Infrastructure Security). Supported versions that are affected are 9.2.0.0-9.2.26.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. While the vulnerability is in JD Edwards EnterpriseOne Tools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all JD Edwards EnterpriseOne Tools accessible data as well as unauthorized access to critical data or complete access to all JD Edwards EnterpriseOne Tools accessible data. CVSS 3.1 Base Score 9.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N).	9.6	More Details
CVE-2026-56073	Cap-go before 12.128.2 contains an authentication bypass vulnerability in OTP verification that allows attackers to bypass email verification by modifying server responses. Attackers can intercept OTP verification requests and manipulate HTTP responses to falsely mark verification successful, enabling unauthorized 2FA enablement and account takeover.	9.4	More Details
CVE-2026-35305	Vulnerability in the Oracle Coherence product of Oracle Fusion Middleware (component: Centralized Third Party Jars). The supported version that is affected is 15.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Coherence. While the vulnerability is in Oracle Coherence, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Coherence accessible data as well as unauthorized update, insert or delete access to some of Oracle Coherence accessible data. CVSS 3.1 Base Score 9.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N).	9.3	More Details
CVE-2026-12048	Stored cross-site scripting in pgAdmin 4's error-rendering and plan-node-rendering paths. Text returned by a PostgreSQL server (ErrorResponse messages, including object names quoted back inside relation-does-not-exist errors and inside EXPLAIN Recheck Cond / Exact Heap Blocks fields) was passed verbatim through html-react-parser at every user-facing sink — the notifier toasts, FormFooterMessage / FormInput help and error areas, FormNote, ModalProvider AlertContent and confirmDelete, ToolErrorView, the Explain visualiser's NodeText panel, the SQL editor confirm dialogs, ConfirmSaveContent, PreferencesHelper modal alerts, and SelectThemes helper text. A PostgreSQL server an attacker controls — or any server returning attacker-influenced text such as a table or column name a low-privilege database user can create — could inject arbitrary HTML (including <iframe>) into the pgAdmin DOM the moment the victim's pgAdmin connected to that server or viewed an Explain plan that referenced the crafted object. The injected iframe's srcdoc could fetch attacker-served JavaScript and, by writing to parent.location, redirect the victim's top-level pgAdmin browser tab to an attacker-controlled URL. Because the injection originates from inside pgAdmin's own interface, standard anti-clickjacking controls (X-Frame-Options, Content-Security-Policy: frame-ancestors) do not mitigate it. A phishing page rendered inside the legitimate pgAdmin window is indistinguishable from a genuine pgAdmin dialog. Fix	9.3	More Details

	combines three complementary layers. (1) DOMPurify sanitisation is wrapped around every html-react-parser call site reachable from notifier, alert, form-error, Explain, and SQL-editor flows. (2) A new plain-text rendering contract — SafeMessage / SafeHtmlMessage components plus Notifier.errorText / alertText / warningText / infoText / successText helpers — is introduced; around fifty callers across browser, tools, dashboard, debugger, misc, llm, preferences, schema diff, and the SQL editor that previously interpolated backend-derived strings are migrated to the plain-text variants. (3) Backend HTML-escape is applied at the post-connection-SQL handler (execute_post_connection_sql) via a new sanitize_external_text helper, so third-party JSON consumers (audit logs, API clients) never receive raw markup either; the Explain plan-info renderer is also patched to _.escape Recheck Cond and Exact Heap Blocks at construction (matching every sibling field), giving defence in depth even before DOMPurify runs. This issue affects pgAdmin 4: from 6.0 before 9.16.		
CVE-2026-39596	Unauthenticated SQL Injection in Blocksy Companion Pro < 2.1.29 versions.	9.3	More Details
CVE-2026-39438	Unauthenticated SQL Injection in ListingPro <= 2.9.10 versions.	9.3	More Details
CVE-2026-46913	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Installation Security). Supported versions that are affected are 9.2.0.0-9.2.26.2. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where JD Edwards EnterpriseOne Tools executes to compromise JD Edwards EnterpriseOne Tools. While the vulnerability is in JD Edwards EnterpriseOne Tools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of JD Edwards EnterpriseOne Tools. CVSS 3.1 Base Score 9.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).	9.3	More Details
CVE-2026-54815	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Cargo RD Cargo Shipping Location for WooCommerce allows Blind SQL Injection. This issue affects Cargo Shipping Location for WooCommerce: from n/a through 5.6.	9.3	More Details
CVE-2026-22332	Unauthenticated SQL Injection in Tutor LMS Pro <= 3.9.6 versions.	9.3	More Details
CVE-2026-22340	Unauthenticated SQL Injection in WPJobster <= 6.3.5 versions.	9.3	More Details
CVE-2026-48875	Unauthenticated SQL Injection in JetSmartFilters <= 3.8.1 versions.	9.3	More Details
CVE-2026-46795	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Content accessible data as well as unauthorized access to critical data or complete access to all Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 9.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:N).	9.3	More Details
CVE-2026-46805	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Content accessible data as well as unauthorized access to critical data or complete access to all Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 9.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:N).	9.3	More Details

CVE-2026-49871	Cross-Site Request Forgery (CSRF) vulnerability in the cas-auth plugin under default configurations. This defect allows a remote attacker that manages to send a victim to a webpage controlled by them can cause the victim's browser to become authenticated as a different identity. Actions the victim takes upstream are then attributed to attackers identity. This issue affects Apache APISIX: from 3.0.0 through 3.16.0. Users are recommended to upgrade to version 3.17.0, which fixes the issue.	9.3	More Details
CVE-2026-54819	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Webilia Inc. Listdom allows Blind SQL Injection. This issue affects Listdom: from n/a through 5.4.0.	9.3	More Details
CVE-2026-55450	Langflow is a tool for building and deploying AI-powered agents and workflows. Prior to 1.9.1, unauthenticated users can upload any amount of data to the server without any limitations. No need for any prior knowledge, only network access to Langflow. This can lead to space exhaustion on the server. In addition, in the response, the absolute path of the uploaded file is reported to the attacker, which is an information leak that can assist in chaining other primitives. This vulnerability is fixed in 1.9.1.	9.3	More Details
CVE-2026-48745	Traccar Client is a GPS tracking mobile app for sending location updates to private servers using the open-source Traccar platform. In versions 9.7.19 and below, a single crafted deep link can silently hijack all GPS tracking parameters and redirect telemetry to an attacker-controlled server. The app registers a custom org.traccar.client://config deep-link scheme that silently writes attacker-supplied parameters (server URL, device ID, accuracy, distance, and interval) into the app's persistent configuration with no confirmation, notification, or visual indication. A single crafted link delivered via SMS, email, a webpage, or any installed app can therefore reconfigure the app the moment the victim taps it, with no special permissions required. As a result, an attacker can covertly redirect all of the victim's GPS telemetry to their own server at maximum precision and frequency, and the change persists across restarts. This gives the attacker continuous, real-time tracking of the victim's location. This issue has been fixed in version 9.7.20.	9.3	More Details
CVE-2026-49076	Unauthenticated SQL Injection in JetEngine <= 3.8.9.1 versions.	9.3	More Details
CVE-2026-54187	Unauthenticated SQL Injection in JetEngine <= 3.8.10.1 versions.	9.3	More Details
CVE-2026-35306	Vulnerability in the Oracle Coherence product of Oracle Fusion Middleware (component: Centralized Third Party Jars). The supported version that is affected is 15.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Coherence. While the vulnerability is in Oracle Coherence, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Coherence accessible data as well as unauthorized update, insert or delete access to some of Oracle Coherence accessible data. CVSS 3.1 Base Score 9.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N).	9.3	More Details
CVE-2026-54808	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WP Travel WP Travel Gutenberg Blocks allows Blind SQL Injection. This issue affects WP Travel Gutenberg Blocks: from n/a through 3.9.4.	9.3	More Details
CVE-2026-46785	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Content accessible data as well as unauthorized access to critical data or complete access to all Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 9.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:N).	9.3	More Details
	TypeBot is a chatbot builder tool. In versions 3.16.1 and earlier, POST /api/blocks/file-input/v3/generate-upload-url is unauthenticated and uses unsanitized fileName input to construct public/ S3 object keys, while issuing presigned PUT URLs that do not bind Content-		

CVE-2026-48768	Type. As a result, any anonymous visitor to a published bot with a file input can upload attacker-controlled HTML, SVG, or JS to attacker-chosen subpaths, including other tenants' publicly served result paths, enabling arbitrary content hosting and potential stored XSS on the storage origin. ../ traversal is blocked by S3/MinIO canonicalization (signature mismatch), but forward-slash path injection is exploitable. This issue has been fixed in version 3.17.0.	9.3	More Details
CVE-2025-59554	Unauthenticated SQL Injection in Advanced Ads – Tracking < 3.0.7 versions.	9.3	More Details
CVE-2026-49079	Unauthenticated SQL Injection in JetSearch <= 3.5.17 versions.	9.3	More Details
CVE-2026-54811	Unauthenticated SQL Injection in WP eMember < v10.9.4 versions.	9.3	More Details
CVE-2026-54186	Unauthenticated SQL Injection in JobSearch <= 3.2.9 versions.	9.3	More Details
CVE-2026-46912	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Web Runtime Security). Supported versions that are affected are 9.2.0.0-9.2.26.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. While the vulnerability is in JD Edwards EnterpriseOne Tools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all JD Edwards EnterpriseOne Tools accessible data as well as unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Tools accessible data. CVSS 3.1 Base Score 9.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N).	9.3	More Details
CVE-2026-54809	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in VillaTheme GIFT4U allows Blind SQL Injection. This issue affects GIFT4U: from n/a through 1.0.10.	9.3	More Details
CVE-2026-49084	Unauthenticated SQL Injection in JetEngine < 3.8.9.1 versions.	9.3	More Details
CVE-2026-54812	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in StylemixThemes Motors allows Blind SQL Injection. This issue affects Motors: from n/a through 1.4.109.	9.3	More Details
CVE-2026-49080	Unauthenticated SQL Injection in wpDataTables <= 7.3.6 versions.	9.3	More Details
CVE-2026-9265	Crypt::OpenSSL::PKCS12 versions before 1.96 for Perl permits a heap OOB read in print_attribute UTF8STRING path. print_attribute() copies a UTF8STRING ASN.1 attribute value into a heap buffer sized exactly to its declared length via strncpy, leaving no NUL terminator. Downstream callers run strlen() on the result and pass the inflated length to newSVpvn(), copying attacker-influenced adjacent heap bytes into a Perl scalar.	9.1	More Details
CVE-2026-46875	Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Deployment Library). Supported versions that are affected are 13.5 and 24.1. Easily exploitable vulnerability allows high privileged attacker with network access via HTTPS to compromise Oracle Enterprise Manager Base Platform. While the vulnerability is in Oracle Enterprise Manager Base Platform, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Manager Base Platform. CVSS 3.1 Base Score 9.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	9.1	More Details
CVE-2026-46892	Vulnerability in the JD Edwards EnterpriseOne Human Resources Management product of Oracle JD Edwards (component: Human Resources). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Human Resources Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all JD Edwards EnterpriseOne Human Resources Management accessible data as well as unauthorized access to critical data or complete access to all JD Edwards EnterpriseOne Human Resources Management accessible data. CVSS 3.1 Base Score	9.1	More Details

	9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).		
CVE-2026-48746	vLLM is an inference and serving engine for large language models (LLMs). From 0.3.0 until 0.22.0, a vulnerability in ASGI web servers and starlette's trust on those web servers enables an authentication bypass of the OpenAI API AuthenticationMiddleware. It allows to use the API without providing the configured VLLM_API_KEY or --api-key. This vulnerability is fixed in 0.22.0.	9.1	More Details
CVE-2026-46858	Vulnerability in the APM - Application Performance Management product of Oracle Enterprise Manager (component: JADM, JVM Diagnostics). Supported versions that are affected are 13.5 and 24.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise APM - Application Performance Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all APM - Application Performance Management accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of APM - Application Performance Management. CVSS 3.1 Base Score 9.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H).	9.1	More Details
CVE-2026-11373	Net::Statsite::Client versions through 1.1.0 for Perl allow metric injections. Net::Statsite::Client is a client for the statsite protocol, which is a variant of statsd. Newlines are not removed from metric names, allowing metric injections. Values are not sanitised for newlines or other protocol control characters such as colons or pipes, allowing metric injections.	9.1	More Details
CVE-2026-46809	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Sites accessible data as well as unauthorized access to critical data or complete access to all Oracle WebCenter Sites accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	9.1	More Details
CVE-2026-12628	IBM Storage Protect Client 8.1.0.0 through 8.2.1.0 and IBM Storage Protect Snapshot For Windows 8.1.0.0 through 8.2.1.0 could allow a remote attacker to bypass authentication due to the use of a hardcoded credential in the FlashCopy Manager (FCM) authentication mechanism. The application contains a static credential embedded in multiple authentication code paths, and does not properly validate authentication responses, which may allow an unauthenticated attacker to establish a trusted session and access protected services. This vulnerability affects client components across multiple versions and may allow an attacker to impersonate legitimate clients, potentially leading to unauthorized access to system resources.	9.1	More Details
CVE-2026-48509	MessagePack for C# is a MessagePack serializer for C#. Prior to 2.5.301 and 3.1.7, the parameterless MessagePackInputFormatter() constructor uses default serializer options, which resolve to MessagePackSerializerOptions.Standard with MessagePackSecurity.TrustedData. The formatter is designed for ASP.NET Core MVC request bodies, which commonly cross an HTTP trust boundary. This insecure default can expose applications to denial-of-service attacks that MessagePackSecurity.UntrustedData is intended to mitigate, such as hash-collision attacks against dictionary-like model properties. This vulnerability is fixed in 2.5.301 and 3.1.7.	9.1	More Details
CVE-2026-56348	n8n before 2.20.0 contains a credential exfiltration vulnerability in the POST /rest/dynamic-node-parameters/options endpoint that allows authenticated users to bypass Allowed HTTP Request Domains restrictions. Attackers with credential access can cause the n8n server to issue HTTP requests with credentials to unauthorized hosts, exfiltrating sensitive authentication data.	9.1	More Details
CVE-2026-9733	Mojolicious::Plugin::Web::Auth::OAuth2 versions through 0.17 for Perl have an insecure default state parameter. When no state generator is specified in the constructor, the module defaults to using a SHA-1 hash of predictable and low-entropy sources, including the epoch time (which is leaked via the HTTP Date header) and a call to Perl's built-in rand function. A predictable state allows an attacker to hijack another user's session through cross site request forgery (CSRF).	9.1	More Details

CVE-2026-46784	Vulnerability in the WebCenter Content: Imaging product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise WebCenter Content: Imaging. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all WebCenter Content: Imaging accessible data as well as unauthorized access to critical data or complete access to all WebCenter Content: Imaging accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	9.1	More Details
CVE-2026-46777	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Content accessible data as well as unauthorized access to critical data or complete access to all Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	9.1	More Details
CVE-2026-35298	Vulnerability in the WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0 and 15.1.1.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise WebLogic Server. While the vulnerability is in WebLogic Server, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of WebLogic Server. CVSS 3.1 Base Score 9.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	9.1	More Details
CVE-2026-35270	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebCenter Content. While the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Content. CVSS 3.1 Base Score 9.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	9.1	More Details
CVE-2026-56081	Cap-go before 12.128.2 contains an authentication logic flaw that lets an attacker register and control an account bound to a victim's email address before that email is verified. By enabling two-factor authentication on the pre-registered account, the attacker gains control over the account claimed under the victim's identity, allowing them to read and modify its state and enforce organization-level policies, while the legitimate user is denied access to the account tied to their own email.	9.1	More Details
CVE-2026-49230	Improper Validation of Integrity Check Value vulnerability in Apache APISIX. The jwe-decrypt plugin under default configuration is vulnerable to authentication bypass. This issue affects Apache APISIX: from 3.8.0 through 3.16.0. Users are recommended to upgrade to version 3.17.0, which fixes the issue.	9.1	More Details
CVE-2026-46896	Vulnerability in the Oracle Enterprise Command Center Framework product of Oracle E-Business Suite (component: Core). Supported versions that are affected are V15 and V16. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Enterprise Command Center Framework. While the vulnerability is in Oracle Enterprise Command Center Framework, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Command Center Framework. CVSS 3.1 Base Score 9.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	9.1	More Details
CVE-2026-	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Enterprise Infrastructure Security). Supported versions that are affected are 9.2.0.0-9.2.26.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all JD	9.1	More

46910	Edwards EnterpriseOne Tools accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of JD Edwards EnterpriseOne Tools. CVSS 3.1 Base Score 9.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H).		Details
CVE-2026-20181	A vulnerability in Cisco ISE and ISE-PIC could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device. To exploit this vulnerability, the attacker must have valid administrative credentials. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to obtain user-level access to the underlying operating system and then elevate privileges to root. In single-node deployments, successful exploitation of this vulnerability could cause the affected ISE node to become unavailable, resulting in a denial of service (DoS) condition. In that condition, endpoints that have not already authenticated would be unable to access the network until the node is restored.	9.1	More Details
CVE-2026-36418	JimuReport versions 2.3.4 and below are vulnerable to remote code execution due to improper handling of Aviator expressions. The /jmreport/executeSelectApi endpoint passes user-supplied input directly to the Aviator expression engine without adequate validation allowing attackers to execute arbitrary code.	9.1	More Details
CVE-2026-20266	In Splunk AI Toolkit versions below 5.7.4, a user who holds the "admin" Splunk role could execute arbitrary OS commands on the host running the Splunk Enterprise instance. The vulnerability is possible because of an unsafe shell execution pattern in the btool configuration helper, which constructs OS command strings from dynamic parameters without disabling shell interpretation.	9.1	More Details
CVE-2026-49268	A remote attacker can inject LDAP special characters into the Distinguished Name (DN) construction in DefaultLdapRealm class. User-supplied username input is directly concatenated into the LDAP DN template without any escaping of RFC 2253 special characters. This allows an attacker to manipulate the DN structure used for LDAP bind authentication, potentially bypassing authentication or impersonating other users. This issue affects all Apache Shiro versions through 2.2.0, and 3.0.0-alpha-1 when using DefaultLdapRealm Upgrade to Apache Shiro 2.2.1 or 3.0.0-alpha-2 or later, which fixes the issue.	9.1	More Details
CVE-2026-55196	Hermes WebUI before 0.51.409 contains an authentication bypass vulnerability in passkey registration endpoints that allows unauthenticated remote attackers to register arbitrary passkeys. When HERMES_WEBUI_PASSKEY=1 is enabled with no existing credentials, POST /api/auth/passkey/register/options and POST /api/auth/passkey/register endpoints are accessible without authentication, allowing attackers to claim the first passkey and gain permanent administrative control.	9.1	More Details
CVE-2026-48814	Network-AI is a TypeScript/Node.js multi-agent orchestrator. In versions 5.7.1 and earlier, the MCP SSE server allows unauthenticated cross-origin MCP tool invocation due to an empty default secret. This issue was partially addressed by CVE-2026-46701 in version 5.4.5 by closing the CORS flaw (with Access-Control-Allow-Origin now set only for localhost origins), but the empty-default-secret flaw described in the title remained: the SSE MCP server still defaulted to an empty secret, _isAuthorized() still returned true when the secret was empty, and a non-loopback bind only produced a warning. As a result, the server still ran fully unauthenticated by default. Any non-browser caller (for example, curl, SSRF, or a 0.0.0.0 bind) could invoke all 22 MCP tools (config_set, agent_spawn, blackboard_write, token_*) with no credentials. This issue was fixed in version 5.7.2.	9.1	More Details
CVE-2026-54387	Tinyproxy through 1.11.3, fixed in commit ff45d3b, fails to reconcile conflicting Content-Length and Transfer-Encoding: chunked headers, forwarding both verbatim to the backend while using Content-Length to determine how many request body bytes to consume. Remote attackers can desynchronize the proxy and backend parser state, allowing injection of arbitrary HTTP requests to the backend to enable cache poisoning, access control bypass, and request hijacking.	9.1	More Details
CVE-2026-54388	Tinyproxy through 1.11.3, fixed in commit 364cdb6, fails to reject requests containing multiple Content-Length headers with differing values, forwarding all duplicate headers to the backend while using the first value to determine how many request body bytes to consume. Remote attackers can desynchronize the proxy and backend parser state, allowing injection of	9.1	More Details

	arbitrary HTTP requests to the backend to enable cache poisoning, access control bypass, and request hijacking.		
CVE-2026-50203	A path traversal in the SFTP provider (`SFTPHook.retrieve_directory` / `SFTPOperator(operation=get)`) let a malicious or compromised remote SFTP server write files outside the configured local destination directory via crafted directory-entry names. No Airflow account is required — the attack surface is any deployment downloading directories from an untrusted SFTP server. Upgrade `apache-airflow-providers-sftp` to 5.8.1 or later.	9.1	More Details
CVE-2026-49454	Relyra is a strict-by-default SAML 2.0 Service Provider library for Elixir and Phoenix. Versions 1.0.0 and 1.1.0 accept forged SAML signatures because SignatureValue was not cryptographically verified before the library returned a successful authentication result. The XMLDSig trust boundary was incomplete as :public_key.verify over the exclusive-C14N canonicalized SignedInfo was not performed against the configured IdP certificate's public key, DigestValue was not recomputed over the canonicalized referenced element, and canonicalize/2 remained an unused passthrough in the signature-verification path. The result was a structure-only acceptance path where document shape and trust-source rejection could succeed without proving the signature bytes. A forged SignatureValue carrying an attacker-controlled NameID could be accepted as {:ok}. This issue has been fixed in version 1.2.0.	9.1	More Details
CVE-2026-24611	Unauthenticated Broken Access Control in MetForm Pro <= 3.9.1 versions.	9.1	More Details
CVE-2026-32967	Incorrect Authorization vulnerability of `/v2` experimental interface in Apache DolphinScheduler. This issue affects Apache DolphinScheduler: before 3.4.2. Users are recommended to upgrade to version 3.4.2, which fixes the issue.	9.1	More Details
CVE-2026-39999	Authentication Bypass by Spoofing vulnerability in Apache APISIX. The attacker can completely bypass authentication capitalising on certain configurations of jwt-auth plugin. This issue affects Apache APISIX: from v2.2 through v3.16.0. Users are recommended to upgrade to version v3.17.0, which fixes the issue.	9.1	More Details
CVE-2026-9142	There is an insecure default credentials vulnerability in NI grpc-device when TLS configuration is not present and the server is bound beyond loopback. This may allow an unauthenticated user access to the server on the local network. This affects NI grpc-device 2.17.0 and prior versions.	9.1	More Details
CVE-2026-8713	The Avada (Fusion) Builder plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the maybe_delete_files function in all versions up to, and including, 3.15.3. This makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php). The attack requires a published Avada form configured to save entries to the database; an unauthenticated attacker submits a path-traversal payload via the wp_ajax_nopriv_fusion_form_submit_ajax handler while also controlling the fusion_privacy_expiration_interval and privacy_expiration_action fields to force an immediate 'delete' cleanup, causing the planted entry to be automatically processed by the Fusion_Form_DB_Privacy shutdown-hook routine without any administrator interaction.	9.1	More Details
CVE-2026-46949	Vulnerability in the Oracle Advanced Outbound Telephony product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Advanced Outbound Telephony. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Advanced Outbound Telephony accessible data as well as unauthorized access to critical data or complete access to all Oracle Advanced Outbound Telephony accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	9.1	More Details
CVE-2026-46946	Vulnerability in the Oracle iSupport product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle iSupport. While the vulnerability is in Oracle iSupport, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle iSupport. CVSS 3.1 Base Score 9.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	9.1	More Details

CVE-2026-46945	Vulnerability in the Oracle iSupport product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle iSupport. While the vulnerability is in Oracle iSupport, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle iSupport. CVSS 3.1 Base Score 9.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	9.1	More Details
CVE-2026-46930	Vulnerability in the Oracle In-Memory Cost Management for Discrete Industries product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.12-12.2.15. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle In-Memory Cost Management for Discrete Industries. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle In-Memory Cost Management for Discrete Industries accessible data as well as unauthorized access to critical data or complete access to all Oracle In-Memory Cost Management for Discrete Industries accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	9.1	More Details
CVE-2026-46944	Vulnerability in the Oracle iSupport product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle iSupport. While the vulnerability is in Oracle iSupport, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle iSupport. CVSS 3.1 Base Score 9.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	9.1	More Details
CVE-2025-62821	Microsoft HEIF Image Extensions 1.2.22.0 has an out-of-bounds read because CHEIFItemInfoEntry_GetDataSize can return success while leaving the reported data size as 0. This causes a caller to make a 1-byte allocation. Later, CopyPixels computes copy_size = stride * abs(roi_height) but does not check the source buffer length before a memmove call.	9.1	More Details
CVE-2026-44087	Insufficient Verification of Data Authenticity vulnerability in Apache APISIX. The openid-connect plugin under default configuration has an attack surface that allows the attacker to spoof identity headers allowing the attacker to get unauthorized access the protected resources. This issue affects Apache APISIX: from 2.3 through 3.16.0. Users are recommended to upgrade to version 3.17.0, which fixes the issue.	9.1	More Details
CVE-2026-48137	There is an untrusted pointer dereference vulnerability in the NI grpc-device sideband streaming API that may allow an attacker to cause an arbitrary memory dereference, potentially resulting in remote code execution. Successful exploitation requires an attacker to supply a specially crafted Moniker protobuf message. This affects NI grpc-device 2.17.0 and prior versions.	9.1	More Details
CVE-2026-54157	LobeHub is a work-and-lifestyle space to find, build, and collaborate with agent teammates that grow with you. Prior to 2.1.57, the /webapi/proxy endpoint on app.lobehub.com accepts a URL in the POST body and fetches it server-side without any authentication. An attacker can use this to make arbitrary outbound requests from LobeHub's infrastructure, leak Vercel deployment details, and inject cookies on the lobehub.com domain through reflected Set-Cookie headers. This vulnerability is fixed in 2.1.57.	9.0	More Details
CVE-2026-46872	Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Install). Supported versions that are affected are 13.5 and 24.1. Easily exploitable vulnerability allows high privileged attacker with network access via HTTPS to compromise Oracle Enterprise Manager Base Platform. While the vulnerability is in Oracle Enterprise Manager Base Platform, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Enterprise Manager Base Platform accessible data as well as unauthorized read access to a subset of Oracle Enterprise Manager Base Platform accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Enterprise Manager Base Platform. CVSS 3.1 Base Score 9.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:H/A:H).	9.0	More Details
	Two state-mutating endpoints in pgAdmin 4's SQL Editor blueprint -- DELETE /sqleditor/close/<trans_id> and POST		

CVE-2026-12046	/sqleditor/initialize/sqleditor/update_connection/<sgid>/<sid>/<did> -- were the only routes in the module missing the @pga_login_required decorator. Both reach a pickle.loads sink on session['gridData'][<trans_id>]['command_obj']: the close endpoint via close_sqleditor_session(), and update_sqleditor_connection via check_transaction_status(). In server mode these endpoints were reachable without any authenticated pgAdmin session. The defect is a missing-authentication-on-critical-function (CWE-306) wrapper around a deserialization-of-untrusted-data sink (CWE-502). Exploiting it for remote code execution requires the attacker to also forge a server-side session file whose gridData entry contains a malicious pickle payload, which in turn requires both (a) knowledge of pgAdmin's Flask SECRET_KEY (no chain to leak it is described here -- the attacker must already possess it) and (b) write access to pgAdmin's sessions/ directory on the host. Neither precondition is granted by this defect on its own. When those preconditions are met from another channel (misconfigured deployment, prior compromise, leaked configuration), the missing auth gate is the final hop that turns an existing partial compromise into unauthenticated code execution in the pgAdmin process -- and, by extension, on the host under whatever account runs pgAdmin. Fix is a one-line @pga_login_required decorator on each of the two endpoints, matching the convention used by every other route in the module. The is_authenticated / MFA chain now runs before the trans_id is dereferenced, so an unauthenticated request is rejected before reaching the deserialization path. The defect is server-mode only. In DESKTOP mode pgAdmin's before_request hook re-authenticates DESKTOP_USER on every request, so no endpoint can be exercised in an unauthenticated state and no auth decorator (or its absence) is meaningful. The accompanying regression test mirrors the attacker's path -- harvests an X-pgA-CSRFToken from GET /login and replays it against both endpoints -- and self-skips outside server mode for that reason; it is wired into the existing server-mode CI workflow alongside the data-isolation tests. This issue affects pgAdmin 4: from 6.9 before 9.16.	9.0	More Details
CVE-2026-35320	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. While the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Content. CVSS 3.1 Base Score 9.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H).	9.0	More Details
CVE-2026-12249	An issue was discovered in Canonical ADSys upstream versions through v0.16.2. During Active Directory Certificate Services (AD CS) certificate auto-enrollment via the vendored Samba client script (internal/policies/certificate/python/vendor_samba/gp/gp_cert_auto_enroll_ext.py), ADSys utilizes a plaintext HTTP connection (http://) instead of a secure HTTPS connection (https://) to request the CA certificate from the Active Directory Certificate Services server (GetCACert). An unauthenticated network attacker positioned between the managed Ubuntu host and the configured AD CS CA hostname can conduct a Man-in-the-Middle (MITM) attack. By intercepting the plaintext HTTP request, the attacker can supply an arbitrary, attacker-controlled Root CA certificate. Because the system automatically accepts this certificate and registers it into the local system trust store via update-ca-certificates, this results in system-wide trust store poisoning. Consequently, TLS clients utilizing the operating system trust store on the affected machine will accept rogue certificates for arbitrary domains, enabling persistent decryption and interception of subsequent TLS connections. This issue is resolved in version v0.16.3.	9.0	More Details
CVE-2026-11374	In ManageEngine ADSelfService Plus, RecoveryManager Plus, M365 Manager Plus, and ADAudit Plus, the SSO tickets generated to authenticate that session could be predicted by an unauthenticated user, leading to account takeover.	9.0	More Details
CVE-2026-52705	Unauthenticated Arbitrary File Upload in SigmaForms Pro – AI Generated Forms <= 1.4.5 versions.	9.0	More Details
	Read-only transaction bypass in the pgAdmin 4 AI Assistant allows an attacker who can influence database content that the assistant reads to execute arbitrary SQL with the privileges of the pgAdmin user's database role. The AI Assistant's execute_sql_query tool runs LLM-generated SQL inside a BEGIN TRANSACTION READ ONLY wrapper to prevent data modification. The LLM-supplied query was forwarded to the database driver without restriction to a single statement or to read-only verbs, so a multi-statement payload beginning with		

CVE-2026-12045	COMMIT, END, ROLLBACK, or ABORT terminated the read-only transaction and ran subsequent statements in autocommit mode. The trailing ROLLBACK then had no effect. Delivery is via prompt injection: an attacker who can write content into any object the AI Assistant may inspect (a row, a column value, a comment) can cause the LLM to emit the multi-statement payload as a tool call. With ordinary write privileges on the pgAdmin user's role the attacker can perform unauthorised data modification. When the pgAdmin user's role is a PostgreSQL superuser or holds pg_execute_server_program, the chain extends to remote code execution on the database server host via COPY ... TO PROGRAM. Fix validates the LLM-supplied query up front: it must parse to exactly one non-empty / non-comment statement whose leading real token (after stripping whitespace, comments, and punctuation) is one of SELECT, WITH, EXPLAIN, SHOW, VALUES, or TABLE. Transaction-control verbs, DML, DDL, CALL, COPY, DO, SET/RESET, and everything else are rejected before any database work happens. PostgreSQL's READ ONLY mode continues to backstop data-modifying CTEs, EXPLAIN ANALYZE on writes, and volatile side effects. This issue affects pgAdmin 4: from 9.13 before 9.16.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2026-55738	A stack-based buffer overflow exists in the raw_to_header() function in src/microtar.c in rxi microtar 0.1.0. The function copies the 100-byte name and linkname fields of a TAR header with strcpy() without guaranteeing null termination of the source. The POSIX ustar format permits these fixed-width fields to be fully populated with non-null bytes, so a crafted archive whose linkname field (followed by the trailing padding of the 512-byte raw header) contains no null terminator causes strcpy() to read past the end of the 512-byte raw header stack buffer and to write past the destination header buffer. A remote attacker who supplies a crafted TAR archive that the victim opens or parses (via mtar_open(), mtar_read_header(), or mtar_find()) can cause an out-of-bounds read and a stack buffer overflow, resulting in denial of service (crash) and potentially arbitrary code execution. Confirmed with AddressSanitizer: stack-buffer-overflow READ of size 356 in raw_to_header at src/microtar.c:112.	8.8	More Details
CVE-2026-46864	Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Agent Next Gen). Supported versions that are affected are 13.5 and 24.1. Easily exploitable vulnerability allows low privileged attacker with network access via SSH to compromise Oracle Enterprise Manager Base Platform. Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Manager Base Platform. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2026-46947	Vulnerability in the Oracle Advanced Outbound Telephony product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Advanced Outbound Telephony. Successful attacks of this vulnerability can result in takeover of Oracle Advanced Outbound Telephony. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2026-46942	Vulnerability in the Oracle Process Manufacturing Process Planning product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Process Manufacturing Process Planning. Successful attacks of this vulnerability can result in takeover of Oracle Process Manufacturing Process Planning. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2026-46940	Vulnerability in the Oracle Cost Management product of Oracle E-Business Suite (component: Cost Planning). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Cost Management. Successful attacks of this vulnerability can result in takeover of Oracle Cost Management. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details

CVE-2026-12806	A vulnerability has been found in Edimax BR-6478AC V2 1.23. The impacted element is the function formWlSiteSurvey of the file /goform/formWlSiteSurvey of the component POST Request Handler. The manipulation of the argument selSSID leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2026-46937	Vulnerability in the Oracle iSetup product of Oracle E-Business Suite (component: General Ledger Update Transform, Reports). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle iSetup. Successful attacks of this vulnerability can result in takeover of Oracle iSetup. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2026-8157	The Vitepos WordPress plugin before 3.4.2 does not properly restrict the roles that can be assigned when creating new users via one of its REST API endpoints, allowing authenticated users with a custom Vitepos WordPress plugin before 3.4.2 role to escalate privileges to administrator.	8.8	More Details
CVE-2026-12165	The Contest Gallery – Upload & Vote Photos, Media, Sell with PayPal & Stripe plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 30.0.2 via the `RegistryUserRole` parameter. This is due to the plugin's admin menu being registered at the `edit_posts` capability level — granting Contributor-level users access to the plugin's admin pages and a valid `cg_admin` nonce — while the option-saving handler in `change-options-and-sizes.php` performs no `current_user_can()` capability check beyond `check_admin_referer('cg_admin')`, and the `RegistryUserRole` value is processed only through `sanitize_text_field()` and `htmlentities()` without restriction to an allowlist of permitted role names. This makes it possible for authenticated attackers, with author-level access and above, to overwrite the plugin's stored `RegistryUserRole` option with `administrator`, which the `cg_create_wp_user_from_google_user` function then reads back from the `contest_gal1ery_registry_and_login_options` database table without any allowlist validation and passes directly to `wp_update_user()`, effectively promoting a newly registered Google sign-in account to Administrator.	8.8	More Details
CVE-2026-12256	Contributor PHP Object Injection in Avada <= 3.15.3 versions.	8.8	More Details
CVE-2026-46931	Vulnerability in the Oracle Enterprise Asset Management product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.6-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Enterprise Asset Management. Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Asset Management. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2026-46929	Vulnerability in the Oracle Cost Management product of Oracle E-Business Suite (component: Cost Planning). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Cost Management. Successful attacks of this vulnerability can result in takeover of Oracle Cost Management. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2026-46928	Vulnerability in the Oracle Spares Management product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise Oracle Spares Management. Successful attacks of this vulnerability can result in takeover of Oracle Spares Management. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2026-46926	Vulnerability in the Siebel CRM Cloud Applications product of Oracle Siebel CRM (component: Siebel Cloud Manager). Supported versions that are affected are 17.0-26.5. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Siebel CRM Cloud Applications executes to compromise Siebel CRM Cloud Applications. While the vulnerability is in Siebel CRM Cloud Applications, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Siebel CRM Cloud Applications. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability	8.8	More Details

	impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).		
CVE-2026-46921	Vulnerability in the Siebel CRM Cloud Applications product of Oracle Siebel CRM (component: Siebel Cloud Manager). Supported versions that are affected are 17.0-26.5. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel CRM Cloud Applications. Successful attacks of this vulnerability can result in takeover of Siebel CRM Cloud Applications. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2026-12439	Use after free in Digital Credentials in Google Chrome prior to 149.0.7827.155 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details
CVE-2026-46916	Vulnerability in the Oracle Process Manufacturing Product Development product of Oracle E-Business Suite (component: Quality Management Specs). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Process Manufacturing Product Development. Successful attacks of this vulnerability can result in takeover of Oracle Process Manufacturing Product Development. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2026-12441	Use after free in File Input in Google Chrome on Linux prior to 149.0.7827.155 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details
CVE-2026-46903	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Business Logic Infrastructure Security). Supported versions that are affected are 9.2.0.0-9.2.26.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in takeover of JD Edwards EnterpriseOne Tools. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2025-59563	Subscriber Privilege Escalation in Sonaar <= 4.27.4 versions.	8.8	More Details
CVE-2026-12443	Use after free in Web Authentication in Google Chrome prior to 149.0.7827.155 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details
CVE-2026-12447	Heap buffer overflow in WebRTC in Google Chrome prior to 149.0.7827.155 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-12448	Inappropriate implementation in WebView in Google Chrome on Android prior to 149.0.7827.155 allowed a remote attacker to perform privilege escalation via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-46886	Vulnerability in the Siebel Apps - Marketing product of Oracle Siebel CRM (component: Marketing). Supported versions that are affected are 17.0-26.5. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel Apps - Marketing. Successful attacks of this vulnerability can result in takeover of Siebel Apps - Marketing. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2026-46885	Vulnerability in the Siebel CRM Integration product of Oracle Siebel CRM (component: EAI). Supported versions that are affected are 17.0-26.5. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel CRM Integration. Successful attacks of this vulnerability can result in takeover of Siebel CRM Integration. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2026-12452	Use after free in Downloads in Google Chrome on Android prior to 149.0.7827.155 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
	A flaw was found in the Windows Machine Config Operator (WMCO) for Red Hat OpenShift		

CVE-2026-54099	Container Platform. The WICD CSR auto-approver validates that a Certificate Signing Request contains the organization system:wicd-nodes but does not reject additional organization values such as system:masters. A compromised Windows worker node that holds WICD credentials can submit a CSR that is auto-approved and signed by the cluster, yielding a client certificate that grants cluster-administrator privileges and enabling full cluster takeover.	8.8	More Details
CVE-2026-46950	Vulnerability in the Oracle Advanced Outbound Telephony product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Advanced Outbound Telephony. Successful attacks of this vulnerability can result in takeover of Oracle Advanced Outbound Telephony. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2026-46951	Vulnerability in the Oracle Quality product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Quality. Successful attacks of this vulnerability can result in takeover of Oracle Quality. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2026-46952	Vulnerability in the Oracle Quality product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Quality. Successful attacks of this vulnerability can result in takeover of Oracle Quality. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2026-47645	Url redirection to untrusted site ('open redirect') in Microsoft 365 Copilot's Business Chat allows an unauthorized attacker to elevate privileges over a network.	8.8	More Details
CVE-2019-25758	Joomla! Component vBizz 1.0.7 contains an unrestricted file upload vulnerability that allows authenticated attackers to upload arbitrary PHP files by submitting malicious files through the profile_pic parameter. Attackers can upload PHP files via POST requests to the employee view endpoint and execute them from the uploads directory to achieve remote code execution.	8.8	More Details
CVE-2026-55741	Cotonti 1.0.0 (master branch, commit f43f1fc3) is vulnerable to Cross-Site Request Forgery in the administration configuration handler. In system/admin/admin.config.php, the configuration update action ('a=update') processes POST data via cot_config_update_options() without calling cot_check_xg() to validate the anti-CSRF token (the 'x' parameter), unlike other admin handlers (e.g. admin.structure.php, admin.cache.php). A remote attacker who lures an authenticated administrator into visiting a malicious page can force the browser to submit a forged request that modifies arbitrary core, module, or plugin configuration options, which can be leveraged to weaken security or enable further compromise.	8.8	More Details
CVE-2026-8163	The Infility Global WordPress plugin before 2.15.19 does not properly sanitize and escape some parameters before using them in SQL statements, leading to a SQL Injection vulnerability exploitable by authenticated users with Subscriber-level access and above.	8.8	More Details
CVE-2025-69138	Subscriber Privilege Escalation in Genemy <= 1.6.6 versions.	8.8	More Details
CVE-2026-10711	Missing authentication for critical function vulnerability in AKIN Software Computer Import Export Industry and Trade Ltd. CafePlus allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects CafePlus: from 12.05.03 before 12.05.04.	8.8	More Details
CVE-2025-69130	Subscriber PHP Object Injection in Entrepreneur - Booking for Small Businesses WordPress Theme <= 3.1.3 versions.	8.8	More Details
CVE-2026-35065	Dell PowerFlex Manager, version(s) [Versions], contain(s) a Missing Authentication for Critical Function vulnerability. An unauthenticated attacker with adjacent network access could potentially exploit this vulnerability, leading to Code execution, Denial of service, Information disclosure, Information tampering, Remote execution, Script injection, and Unauthorized access.	8.8	More Details

CVE-2026-54232	vLLM is an inference and serving engine for large language models (LLMs). Prior to 0.22.1, the vLLM Dockerfile is vulnerable to a dependency confusion attack through the flashinfer-jit-cache package. The package is installed from a custom index (flashinfer.ai/whl/) using --extra-index-url, but the package name was not registered on PyPI, and UV_INDEX_STRATEGY="unsafe-best-match" is set globally. An attacker who registers flashinfer-jit-cache on PyPI with version 0.6.11.post2 can execute arbitrary code as root during the Docker build and backdoor every resulting container image, enabling exfiltration of all user prompts, API credentials, and model data from production vLLM deployments This vulnerability is fixed in 0.22.1.	8.8	More Details
CVE-2026-35018	NetComm NF20MESH routers running firmware R6B031 and earlier contain an authenticated remote code execution vulnerability that allows authenticated attackers to execute arbitrary commands as root by injecting shell metacharacters into the username JSON parameter processed by the dalStorage_addUserAccount function. Attackers can exploit the unsafe concatenation of user-supplied input into a shell command string passed to rut_doSystemAction without sanitization to achieve full root-level command execution on the underlying operating system.	8.8	More Details
CVE-2025-66391	In Citrix Cloud through 2025-11-10, an account with read-only access can trigger the beginning of a workflow for write operations, e.g., the system will send a one-time password to an attacker-controlled email address when the attacker attempts to reset the password of a user account.	8.8	More Details
CVE-2026-32208	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Edge (Chromium-based) allows an authorized attacker to perform spoofing over a network.	8.8	More Details
CVE-2026-54805	Subscriber Privilege Escalation in Falang multilanguage <= 1.4.2 versions.	8.8	More Details
CVE-2026-56396	phpMyFAQ before 4.1.4 contains missing authorization vulnerabilities in editUser() and updateUserRights() endpoints that allow authenticated administrators to escalate privileges. Non-SuperAdmin users with edit_user permission can set is_superadmin flag or grant arbitrary rights to escalate to SuperAdmin access.	8.8	More Details
CVE-2026-56216	Capgo before 12.128.2 contains a scope escalation vulnerability in the POST /functions/v1/apikey endpoint that allows app-limited API keys to mint unrestricted keys by setting empty limits. Attackers with a compromised app-limited key can create an unrestricted key with org-wide access to resources like app listings and other protected endpoints.	8.8	More Details
CVE-2026-56340	vLLM versions >= 0.10.2 and < 0.13.0 are missing sparse tensor validation in multimodal embeddings processing. Because PyTorch disables sparse tensor invariant checks by default, an attacker can submit crafted embedding requests with malformed (negative or out-of-bounds) tensor indices, when the prompt-embeds feature is enabled, to trigger crashes or resource exhaustion (denial of service), with potential for out-of-bounds/write-what-where memory corruption. This continues CVE-2025-62164, whose prior fix only disabled the feature by default rather than addressing the root cause.	8.8	More Details
CVE-2026-46973	Vulnerability in the Oracle Outsourced Mfg for Discrete Industries product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Outsourced Mfg for Discrete Industries. Successful attacks of this vulnerability can result in takeover of Oracle Outsourced Mfg for Discrete Industries. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2026-46972	Vulnerability in the Oracle Outsourced Mfg for Discrete Industries product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Outsourced Mfg for Discrete Industries. Successful attacks of this vulnerability can result in takeover of Oracle Outsourced Mfg for Discrete Industries. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2025-71322	PickleScan before 0.0.33 fails to include the pty.spawn function in its unsafe globals list, allowing attackers to bypass security checks. Malicious actors can craft pickle payloads using pty.spawn to achieve arbitrary code execution when files are processed by PickleScan.	8.8	More Details

CVE-2026-33760	Langflow is a tool for building and deploying AI-powered agents and workflows. Prior to 1.9.0, Langflow's /api/v1/monitor router exposes 7 endpoints that perform read, write, and delete operations on user-owned resources — messages, sessions, build artifacts, and LLM transaction logs — without verifying that the authenticated requester owns the targeted resource. Any authenticated user can read, modify, rename, or permanently delete another user's data by supplying the target's resource ID or flow_id. This is a classic IDOR/BOLA vulnerability. Notably, the same source file (monitor.py) contains one correctly-implemented endpoint that uses an ownership check, demonstrating the correct pattern was known but inconsistently applied. This vulnerability is fixed in 1.9.0.	8.8	More Details
CVE-2026-46967	Vulnerability in the Oracle Public Sector Financials (International) product of Oracle E-Business Suite (component: Authorization). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Public Sector Financials (International). Successful attacks of this vulnerability can result in takeover of Oracle Public Sector Financials (International). CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2026-46965	Vulnerability in the Oracle Universal Work Queue product of Oracle E-Business Suite (component: Work Provider Site Level Administration). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Universal Work Queue. Successful attacks of this vulnerability can result in takeover of Oracle Universal Work Queue. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2026-46962	Vulnerability in the Oracle Project Portfolio Analysis product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Project Portfolio Analysis. Successful attacks of this vulnerability can result in takeover of Oracle Project Portfolio Analysis. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2026-46961	Vulnerability in the Oracle Project Portfolio Analysis product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Project Portfolio Analysis. Successful attacks of this vulnerability can result in takeover of Oracle Project Portfolio Analysis. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2026-42629	Unauthenticated Broken Authentication in PowerPack Pro for Elementor < v2.13.0 versions.	8.8	More Details
CVE-2026-56423	MISP Core contained broken access-control checks in the bulk deletion flows for Event Reports and Sharing Groups. The affected deleteSelection handlers authorized deletion using broad role-level permissions instead of validating authorization for each selected object. For Event Reports, EventReportsController::deleteSelection relied on the global perm_add capability rather than a per-report ownership/authorization check. As a result, a contributor-level user could submit report IDs or UUIDs for reports belonging to other organisations and hard-delete them instance-wide. The fix changed the callback to call EventReport::fetchIfAuthorized($user, $itemId, 'delete') for each selected report before deletion. For Sharing Groups, SharingGroupsController::deleteSelection relied on the global perm_sharing_group capability rather than verifying ownership of each selected sharing group. This allowed a sharing-group-capable user to hard-delete sharing groups owned by other organisations, bypassing the per-object ownership gate used by the single-object delete action. The fix changed the callback to call SharingGroup::checkIfOwner($user, $itemId) for each selected sharing group. An authenticated attacker with the relevant broad role permission could abuse the affected bulk deletion endpoints to delete objects outside their organisation’s authorization scope, causing loss of event-report content or sharing-group configuration across the instance.	8.8	More Details
CVE-2026-12442	Use after free in Passwords in Google Chrome on Android prior to 149.0.7827.155 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details

CVE-2026-44272	Dell Wyse Management Suite (WMS), versions prior to WMS 2605, contain an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Unauthorized access.	8.8	More Details
CVE-2026-35317	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Content. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2026-46780	Vulnerability in the WebCenter Content: Imaging product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise WebCenter Content: Imaging. Successful attacks of this vulnerability can result in takeover of WebCenter Content: Imaging. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2026-12407	The E2Pdf – Export Pdf Tool for WordPress plugin for WordPress is vulnerable to Missing Authorization in versions up to, and including, 1.32.26. This is due to the screen_action() function lacking a dedicated capability check and nonce verification — when invoked via the ?action=screen routing path the controller's index_action() nonce gate is bypassed entirely — while reading an attacker-controlled option name and value from $_POST['wp_screen_options'] and passing them directly to update_option() with no allowlist, relying solely on the page-level e2pdf_templates capability which the plugin's own Permissions UI allows administrators to grant to any role including Subscriber, Contributor, Author, or Editor. This makes it possible for authenticated attackers, with a custom role that has been granted the e2pdf_templates capability, to overwrite arbitrary WordPress options such as default_role and thereby escalate their privileges to administrator.	8.8	More Details
CVE-2026-22342	Unauthenticated Cross Site Request Forgery (CSRF) in WordPress Dating Theme <= 11.2.0 versions.	8.8	More Details
CVE-2026-55237	AutoGPT is a workflow automation platform for creating, deploying, and managing continuous artificial intelligence agents. Versions prior to 0.6.62 have a DOM-based Cross-Site Scripting (XSS) vulnerability in AutoGPT's signup page. The application improperly trusts a URL parameter (`next`), which is passed to `router.push`. An attacker can craft a malicious link that, when opened by an authenticated user, performs a client-side redirect and executes arbitrary JavaScript in the context of their browser. This could lead to credential theft, internal network pivoting, and unauthorized actions performed on behalf of the victim. Version 0.6.62 patches the issue.	8.8	More Details
CVE-2026-35325	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Content. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2026-35324	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Content. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2026-35322	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Content. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details

CVE-2026-35318	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Sites. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2026-35315	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Content. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2026-56075	PraisonAI before 4.5.128 contains an arbitrary shell command execution vulnerability where the UI modules hardcode approval_mode to auto, overriding administrator configuration from PRAISON_APPROVAL_MODE environment variable. Authenticated attackers can instruct the LLM agent to execute arbitrary shell commands via subprocess.run with shell=True, bypassing the manual approval gate and insufficient command sanitization blocklists.	8.8	More Details
CVE-2026-41862	Spring Statemachine's Kryo-based persistence backends (JPA, MongoDB, Redis and ZooKeeper) deserialise persisted state-machine contexts without enforcing a class allowlist (CWE-502, deserialisation of untrusted data), which can lead to remote code execution inside the application JVM. Affected versions: Spring Statemachine 4.0.0 through 4.0.1 Spring Statemachine 3.2.0 through 3.2.4	8.8	More Details
CVE-2026-35311	Vulnerability in the WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise WebLogic Server. Successful attacks of this vulnerability can result in takeover of WebLogic Server. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2026-35303	Vulnerability in the WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise WebLogic Server. Successful attacks of this vulnerability can result in takeover of WebLogic Server. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2026-8461	An out-of-bounds write vulnerability in FFmpeg's libavcodec library, specifically in the MagicYUV decoder, allows denial-of-service and, in some cases, can be exploited for remote code execution. This vulnerability is associated with the file libavcodec/magicyuv.C. This issue affects FFmpeg before version 8.1.2.	8.8	More Details
CVE-2026-35299	Vulnerability in the WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise WebLogic Server. Successful attacks of this vulnerability can result in takeover of WebLogic Server. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2026-54104	The U.S. Government Accountability Office (GAO) Electronic Protest Docketing System (EPDS) and Civilian Board of Contract Appeals (CBCA) Electronic Docketing System (EDS) trusts client-provided values for the 'epds_role_id' parameter without verification, allowing a remote, authenticated attacker to escalate their own privileges.	8.8	More Details
CVE-2026-46580	In Eclipse Theia versions prior to 1.71.0, files matching the pattern .prompts/*.prompttemplate in a workspace were automatically loaded and could override or extend the AI agent's system prompts. An attacker could craft a malicious repository containing prompt template files that, when the workspace was opened in Theia, replaced the AI's system instructions with attacker-controlled content (indirect prompt injection). Combined with other AI chat features available in untrusted workspaces, this enabled attack chains leading to data exfiltration via Markdown image rendering or arbitrary command execution via task definitions.	8.8	More Details

CVE-2026-44688	In Eclipse Theia versions prior to 1.71.0, the AI chat agent processed workspace file and directory names as part of its prompt context without distinguishing them from system instructions. An attacker could craft a malicious repository with adversarial directory or file names that, when analyzed by the AI agent, would cause the agent to follow attacker-controlled instructions (indirect prompt injection). Combined with other AI chat features available in untrusted workspaces, this enabled attack chains leading to data exfiltration via Markdown image rendering or arbitrary command execution via task definitions.	8.8	More Details
CVE-2026-56424	MISP core contained multiple broken access-control flaws where authorization checks were performed against the wrong entity, or where ownership/editability checks were missing on write paths. In affected subsystems, a lower-privileged authenticated user with the relevant feature permission could cause the application to authorize one object but mutate another, or could modify objects that were merely visible rather than editable by the user's organization. The affected paths included: * Event Reports tag removal: the route-authorized report could differ from the report ID used for tag detachment, enabling cross-organization tag removal from another event report * Collection Elements bulk deletion: bulk deletion authorized against a collection whose ID matched the collection-element row ID, rather than the element's actual parent collection, enabling deletion of elements from collections the user did not own. * Analyst Data capture/update: nested analyst data updates could overwrite an existing record without applying the normal canEditAnalystData ownership check, enabling cross-organization overwrite of analyst data records. * Template Elements editing: editing authorized against a template whose ID matched the template-element ID, rather than the element's actual parent template, enabling unauthorized edits to another organization's template elements. * Decaying Model editing and mappings: write paths loaded models using view-scope access but did not verify edit ownership, enabling users to edit or remap visible models owned by another organization. Successful exploitation could allow an authenticated user with subsystem-specific permissions to perform unauthorized cross-organization modifications or deletions of MISP data, resulting in integrity loss, unauthorized tampering with shared intelligence, and disruption of analyst workflows.	8.8	More Details
CVE-2026-44691	In Eclipse Theia versions prior to 1.69.0, custom task definitions in workspace files (e.g. .theia/tasks.json, .vscode/tasks.json) could be executed without requiring workspace trust. An attacker could craft a malicious repository that, when cloned and opened in Theia, leads to execution of arbitrary commands with the user's privileges. In combination with AI chat features and a workspace .theia/settings.json that disabled tool confirmation, this could be triggered automatically by sending a message in the AI chat.	8.8	More Details
CVE-2026-35265	Vulnerability in the Identity Manager product of Oracle Fusion Middleware (component: Security). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Identity Manager. Successful attacks of this vulnerability can result in takeover of Identity Manager. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2026-9860	The Offload, AI & Optimize with Cloudflare Images plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 1.10.2 via the 'account-id' parameter parameter. This is due to insufficient privilege enforcement on the cf_images_do_setup AJAX handler, which requires only the upload_files capability (Author+) rather than manage_options before writing to wp-config.php, combined with the absence of single-quote escaping — sanitize_text_field() does not strip single quotes, and filter_input(INPUT_POST) bypasses wp_magic_quotes() slashing — allowing a single quote in the account-id or api-key parameter to break out of the single-quoted PHP string literal in the write_config() define() statement. This makes it possible for authenticated attackers, with author-level access and above, to execute code on the server. This is possible because the 'cf-images-nonce' nonce required by the AJAX handler is exposed to all Author-level and above users on wp-admin/upload.php via the CFImages JavaScript object, meaning any upload-capable user can satisfy the nonce check and reach the vulnerable wp-config.php write path.	8.8	More Details
CVE-2026-39998	Improper Input Validation vulnerability in Apache APISIX. The attacker can take advantage of certain configuration in forward-auth plugin to spoof identity headers. This issue affects Apache APISIX: from 2.12.0 through 3.16.0. Users are recommended to upgrade to version 3.17.0, which fixes the issue.	8.8	More Details
	Vulnerability in the Identity Manager product of Oracle Fusion Middleware (component: REST WebServices). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily		

CVE-2026-35267	exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Identity Manager. Successful attacks of this vulnerability can result in takeover of Identity Manager. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2026-12466	Heap buffer overflow in WebRTC in Google Chrome on Windows prior to 149.0.7827.155 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2026-56078	PraisonAI before 1.5.115 contains a path traversal vulnerability in MultiAgentMonitor that fails to sanitize agent IDs when building file paths. Attackers can include traversal sequences like ../ in agent IDs to read, write, or overwrite arbitrary files, enabling sensitive disclosure, denial of service, or code execution.	8.8	More Details
CVE-2026-35259	Vulnerability in the WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 14.1.2.0.0 and 15.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise WebLogic Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of WebLogic Server. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2026-12044	SQL injection in pgAdmin 4 across every dialog template that renders ``COMMENT ON ... IS '<description>'`` for a user-supplied description field. The Jinja templates for Domains (and their constraints), Foreign Tables, Languages, and Event Triggers, plus the Views OID-lookup query, interpolated the description directly inside a single-quoted SQL literal -- ``'{{ data.description }}'`` -- instead of passing it through the ``qtLiteral`` escape filter. An authenticated pgAdmin user with permission to create or alter the affected object types could submit a description containing an apostrophe, break out of the literal and chain arbitrary SQL. The injected SQL runs under the PostgreSQL role the user is already authenticated as; for a connected role with ``COPY ... TO/FROM PROGRAM`` (typically PostgreSQL superuser), this chains to OS command execution on the PostgreSQL host. The defect does not cross a privilege boundary -- the user already has direct SQL access to that role through pgAdmin's Query Tool -- so the attacker gains no capability beyond what their database role already grants. The marginal impact captures bypass of any application-layer Query Tool gating an operator may have configured. The defect was originally reported against the Domain Dialog ``description`` field; a code-wide audit identified sixteen sites of the same pattern across the templates listed above. The same review also surfaced ten related sinks in the pgstattuple/pgstatindex stats templates -- ``pgstattuple('{{schema}}.{{table}}')`` and the matching pgstatindex shape -- where ``qtIdent`` escapes embedded double quotes inside the identifier but not apostrophes, so a user with CREATE privilege on a schema could plant a table or index named ``foo'bar`` and a later stats viewer would render an unbalanced literal. Fix is layered: 1. Sites: replace every ``'{{ x.description }}'`` with ``{{ x.description|qtLiteral(conn) }}`` (no surrounding quotes -- the filter wraps the value in escaped quotes itself). Plumb ``conn=self.conn`` through every ``render_template`` call that loads one of these templates. Also corrects a ``{ % elif`` Jinja typo in the foreign-table schema diff (dead branch). Rewrite the ten pgstattuple/pgstatindex stats sites to address the relation via OID + ``::oid::regclass`` cast (e.g. ``pgstattuple({{ tid }}::oid::regclass)``), eliminating the embedded literal-call form entirely so that bug-class can no longer recur there. 2. Driver hardening: ``qtLiteral`` (in ``utils/driver/psycopg3/__init__.py``) used to silently return the raw unescaped value when its ``conn`` argument was falsy. It now raises ``ValueError`` -- surfacing the entire bug class going forward. The change immediately uncovered eight latent plumbing bugs (in ``schemas/__init__.py``, ``schemas/functions/__init__.py``, ``schemas/tables/utils.py``, ``foreign_servers/__init__.py``, and seven sites in ``roles/__init__.py``) -- all fixed as part of this patch. The inner ``except`` block that swallowed adapter-level failures and returned the raw value is also removed, so unadaptable inputs raise instead of leaking unescaped values. 3. Regression tests: a per-template behavioural test renders each previously-vulnerable template with an apostrophe-injection payload and asserts the escaped fragment is present and the vulnerable fragment absent; a lint test walks every ``*.sql`` template flagging any ``'{{ ... }}'`` single-quote-wrapped interpolation against an explicit allowlist; unit tests cover the new qtLiteral fail-fast and inner-except raise paths. This issue affects pgAdmin 4: from 1.0 before 9.16.	8.8	More Details
	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). The supported version that is affected is 14.1.2.0.0. Easily exploitable		

CVE-2026-46804	vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Content accessible data as well as unauthorized access to critical data or complete access to all Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 8.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:N).	8.7	More Details
CVE-2026-35271	Vulnerability in the PeopleSoft Enterprise PT PeopleTools product of Oracle PeopleSoft (component: Weblogic). Supported versions that are affected are 8.61 and 8.62. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PT PeopleTools. While the vulnerability is in PeopleSoft Enterprise PT PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all PeopleSoft Enterprise PT PeopleTools accessible data as well as unauthorized access to critical data or complete access to all PeopleSoft Enterprise PT PeopleTools accessible data. CVSS 3.1 Base Score 8.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:N).	8.7	More Details
CVE-2026-35258	Vulnerability in the WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 14.1.2.0.0 and 15.1.1.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in WebLogic Server, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all WebLogic Server accessible data as well as unauthorized access to critical data or complete access to all WebLogic Server accessible data. CVSS 3.1 Base Score 8.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:N).	8.7	More Details
CVE-2026-54011	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.6,Open WebUI renders Mermaid blocks from Markdown files in the file preview panel and inserts the generated SVG into the DOM using innerHTML. Because Mermaid is configured with securityLevel: 'loose', attacker-controlled Mermaid content can be rendered unsafely in this flow. A working payload was validated through the Markdown preview path, resulting in JavaScript execution in the victim’s browser under the application origin. This vulnerability is fixed in 0.9.6.	8.7	More Details
CVE-2026-48716	nanobot is a personal AI assistant. In versions 0.1.5.post3 and prior, the WhatsApp bridge in bridge/src/whatsapp.ts constructs a filesystem path using the fileName field from an incoming WhatsApp document message without sanitization. The WhatsApp bridge downloads media attachments and writes them to disk using a filename derived from the sender's message via documentMessage.fileName, which is concatenated with a prefix and its raw value is passed directly to path.join(mediaDir, outFilename). Node.js path.join resolves .. components, allowing an attacker to escape the intended media/ directory by sending a document with a crafted fileName such as ../../../.ssh/authorized_keys. Because the attacker also controls the file content (the downloaded buffer), this is a write-anywhere primitive — both path and content are attacker-controlled. A fix for this issue is planned for version 0.1.5.post4.	8.7	More Details
CVE-2026-46808	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Content accessible data as well as unauthorized access to critical data or complete access to all Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 8.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:N).	8.7	More Details
	DoS Vulnerability in 10G iSCSI Interface of Hitachi Virtual Storage Platform. This issue affects Hitachi Virtual Storage Platform E990, E1090, E1090H: before DKCMAIN Ver.93-07-21-80/00-05, CHB(iSCSI) Ver.88-01-02-04, before DKCMAIN Ver.93-07-01-80/00-07, CHB(iSCSI) Ver.88-01-02-04, before DKCMAIN Ver.93-06-82-80/00-06, CHB(iSCSI) Ver.88-01-02-04, before DKCMAIN		

CVE-2025-7737	Ver.93-06-63-80/00-04, CHB(iSCSI) Ver.88-01-02-04; Hitachi Virtual Storage Platform E390, E590, E790, E390H, E590H, E790H: before DKCMAIN Ver.93-07-21-x0/00-05, CHB(iSCSI) Ver.88-01-02-04, before DKCMAIN Ver.93-07-01-x0/00-07, CHB(iSCSI) Ver.88-01-02-04, before DKCMAIN Ver.93-06-82-x0/00-06, CHB(iSCSI) Ver.88-01-02-04, before DKCMAIN Ver.93-06-63-x0/00-04, CHB(iSCSI) Ver.88-01-02-04, before DKCMAIN Ver.93-07-24-x0/00-02, CHB(iSCSI) Ver.88-01-02-04, before DKCMAIN Ver.93-07-02-x0/00-02, CHB(iSCSI) Ver.88-01-02-04; Hitachi Virtual Storage Platform G130, G150, G350, G370, G700, G900, F350, F370, F700, F900: before DKCMAIN Ver.88-08-10-x0/00-05, CHB(iSCSI) Ver.88-01-02-04; Hitachi Virtual Storage Platform G100, G200, G400, G600, G800, F400, F600, F800: before DKCMAIN Ver.83-06-20-x0/00-05, CHB(iSCSI) Ver.83-01-01-29; Hitachi Virtual Storage Platform VX8, 5100, 5500, 5100H, 5500H, 5200, 5600, 5200H, 5600H: before DKCMAIN Ver.90-09-01-00/01-01, CHB(iSCSI) Ver.90-01-01-07, before DKCMAIN Ver.90-08-83-00/01-01, CHB(iSCSI) Ver.90-01-01-07, before DKCMAIN Ver.90-08-63-00/01-01, CHB(iSCSI) Ver.90-01-01-07; Hitachi Virtual Storage Platform VX7, G1000, G1500, F1500: before DKCMAIN Ver.80-06-93-00/00-04, ISFC Ver.80-01-17.	8.6	More Details
CVE-2025-69128	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in EMV JobCareer allows Path Traversal. This issue affects JobCareer: from n/a through 7.3.	8.6	More Details
CVE-2025-69139	Unauthenticated Arbitrary File Deletion in Car Zone <= 3.7 versions.	8.6	More Details
CVE-2026-53755	Crawl4AI is an open-source LLM friendly web crawler & scraper. Prior to 0.8.9, the Docker API server applied its SSRF destination check to the crawl target URL only, not to the proxy address. An unauthenticated request could supply a proxy pointing at an internal IP and route the browser through it, reaching internal services and cloud-metadata endpoints, while using a perfectly valid crawl URL. The Docker API is unauthenticated by default. /crawl, /crawl/stream, and /crawl/job accept a browser_config (and crawler_config). The following all feed Chromium's egress and were unchecked: browser_config.proxy_config.server, browser_config.proxy (deprecated field), crawler_config.proxy_config.server, and --proxy-server / --proxy-pac-url / --proxy-bypass-list / --host-resolver-rules flags in browser_config.extra_args. This vulnerability is fixed in 0.8.9.	8.6	More Details
CVE-2026-56266	Crawl4AI before 0.8.7 contains a server-side request forgery vulnerability in the /crawl, /crawl/stream, /md, and /llm endpoints that fetch arbitrary user-supplied URLs without validation. Unauthenticated attackers can bypass the internal-address blocklist using IPv6-mapped IPv4 addresses to reach internal services and cloud metadata endpoints.	8.6	More Details
CVE-2026-27400	Unauthenticated Arbitrary File Deletion in BookPro <= 1.1.0 versions.	8.6	More Details
CVE-2026-22343	Unauthenticated Broken Access Control in WordPress Dating Theme <= 11.2.0 versions.	8.6	More Details
CVE-2026-46776	Vulnerability in the Oracle Unified Directory product of Oracle Fusion Middleware (component: OUD Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via LDAP to compromise Oracle Unified Directory. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Unified Directory accessible data as well as unauthorized read access to a subset of Oracle Unified Directory accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Unified Directory. CVSS 3.1 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L).	8.6	More Details
CVE-2026-46915	Vulnerability in the Oracle Complex Maintenance, Repair and Overhaul product of Oracle E-Business Suite (component: Production). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair and Overhaul. While the vulnerability is in Oracle Complex Maintenance, Repair and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Complex Maintenance, Repair and Overhaul. CVSS 3.1 Base Score 8.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H).	8.5	More Details

CVE-2026-22335	Subscriber SQL Injection in WooCommerce Frontend Manager – Ultimate < 6.7.7 versions.	8.5	More Details
CVE-2026-54813	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Brainstorm Force SureDash allows Blind SQL Injection. This issue affects SureDash: from n/a through 1.8.0.	8.5	More Details
CVE-2026-46870	Vulnerability in the MySQL Shell product of Oracle MySQL (component: Shell for VS Code). The supported version that is affected is 2026.2.0+9.6.1. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Shell. While the vulnerability is in MySQL Shell, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of MySQL Shell. CVSS 3.1 Base Score 8.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H).	8.5	More Details
CVE-2026-54818	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in VeronaLabs Slimstat Analytics allows Blind SQL Injection. This issue affects Slimstat Analytics: from n/a through 5.4.11.	8.5	More Details
CVE-2026-49113	Subscriber Arbitrary Code Execution in Cornerstone < 7.8.8 versions.	8.5	More Details
CVE-2025-69135	Subscriber SQL Injection in Events Schedule - WordPress Events Calendar Plugin <= 2.7.2 versions.	8.5	More Details
CVE-2026-54185	Subscriber SQL Injection in Cornerstone < 7.8.8 versions.	8.5	More Details
CVE-2026-54008	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.6, backend/open_webui/utils/oauth.py::_process_picture_url calls validate_url(picture_url) on the initial URL only, then invokes aiohttp.ClientSession.get(picture_url, ...) without allow_redirects=False. aiohttp's default is allow_redirects=True, max_redirects=10; the function does not pass the project's AIOHTTP_CLIENT_ALLOW_REDIRECTS env constant either. An attacker with a valid OAuth IdP identity can therefore submit a public URL that 302-redirects to an internal address and read the internal response body via the attacker's own profile_image_url field. This vulnerability is fixed in 0.9.6.	8.5	More Details
CVE-2026-56012	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in David Lingren Media LIbrary Assistant allows Blind SQL Injection. This issue affects Media LIbrary Assistant: from n/a through 3.35.	8.5	More Details
CVE-2026-49073	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in wpWax Directorist Booking allows Blind SQL Injection. This issue affects Directorist Booking: from n/a through 3.0.3.	8.5	More Details
CVE-2026-48967	Subscriber SQL Injection in Geo Mashup <= 1.13.19 versions.	8.5	More Details
CVE-2026-46788	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Content. CVSS 3.1 Base Score 8.4 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:H).	8.4	More Details
	Vulnerability in the PeopleSoft Enterprise PT PeopleTools product of Oracle PeopleSoft		

CVE-2026-35272	(component: Deployment Package). Supported versions that are affected are 8.61 and 8.62. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where PeopleSoft Enterprise PT PeopleTools executes to compromise PeopleSoft Enterprise PT PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PT PeopleTools. CVSS 3.1 Base Score 8.4 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	8.4	More Details
CVE-2026-54320	Daytona is a secure and elastic infrastructure runtime for AI-generated code execution and agent workflows. Prior to 0.184.0, organization invitations could be accepted (and declined) by a user whose email matched the invitation but had not been verified. Daytona authenticates users via OIDC and matches an invitation's target email against the email in the caller's token, but the invitation accept and decline paths did not require that email to be verified, unlike organization creation, which already enforced verification. On identity providers that allow self-service signup and issue a session before the email is verified, an actor could register an address matching a pending invitation, leave it unverified, and accept the invitation, joining the target organization with the role the invitation carried (up to Owner). This vulnerability is fixed in 0.184.0.	8.4	More Details
CVE-2025-26240	In JazzCore python-pdfkit 1.0.0, the from_string method enables the execution of JavaScript code within the context of the server application and the exfiltration of local files.	8.4	More Details
CVE-2024-32949	Missing Authorization vulnerability in Prince Integrate Google Drive allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Integrate Google Drive: from n/a through 1.3.8.	8.3	More Details
CVE-2026-35262	Vulnerability in the Oracle Data Integrator product of Oracle Fusion Middleware (component: Market Place). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Data Integrator. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Data Integrator accessible data as well as unauthorized access to critical data or complete access to all Oracle Data Integrator accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Data Integrator. CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L).	8.3	More Details
CVE-2026-56225	Capgo before 12.128.2 contains an authorization bypass vulnerability in its public API key management handlers (get/put/delete/post). API keys created with mode=all but restricted to a single app via limited_to_apps are only checked for limited_to_orgs and not for limited_to_apps, so an app-scoped key can enumerate, update, and delete sibling API keys belonging to the same account that are outside its declared app scope, enabling tampering with account-level credentials.	8.3	More Details
CVE-2026-50574	yt-dlp is a command-line audio/video downloader. Prior to 2026.06.09, if aria2c is used as an external downloader for a fragmented manifest format (such as an HLS/DASH stream), yt-dlp passes insufficiently sanitized input to aria2c that allows an attacker to perform an arbitrary file write. On Windows platforms, this can lead to immediate arbitrary code execution. On non-Windows platforms, this can lead to arbitrary code execution upon the next invocation of yt-dlp. This vulnerability is fixed in 2026.06.09.	8.3	More Details
CVE-2026-56215	Capgo before 12.128.12 allows authenticated users to modify their mutable public.users.email to arbitrary addresses, which the SSO provisioning endpoint trusts as an account-merge key. Attackers can pre-position their account with a victim's corporate SSO email, causing the provision-user endpoint to merge the victim's SSO identity into the attacker-controlled account.	8.3	More Details
CVE-2026-12468	Race in Updater in Google Chrome on Mac prior to 149.0.7827.155 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-12464	Use after free in Browser in Google Chrome prior to 149.0.7827.155 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-12454	Race in Safe Browsing in Google Chrome on Mac prior to 149.0.7827.155 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details

CVE-2026-12465	Object lifecycle issue in Metrics in Google Chrome prior to 149.0.7827.155 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-12451	Use after free in DigitalCredentials in Google Chrome prior to 149.0.7827.155 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-54010	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.6, Open WebUI lets an authenticated user attach arbitrary file_id values to their own chat message without checking whether they own or can read those files. If the attacker then shares that chat and grants themselves read access, has_access_to_file() treats the victim file as accessible through the shared chat, and the file endpoints read or delete the victim file. This vulnerability is fixed in 0.9.6.	8.3	More Details
CVE-2026-12467	Use after free in Extensions in Google Chrome prior to 149.0.7827.155 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	8.3	More Details
CVE-2026-46925	Vulnerability in the Siebel CRM Cloud Applications product of Oracle Siebel CRM (component: Siebel Cloud Manager). Supported versions that are affected are 17.0-26.5. Difficult to exploit vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Siebel CRM Cloud Applications executes to compromise Siebel CRM Cloud Applications. While the vulnerability is in Siebel CRM Cloud Applications, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Siebel CRM Cloud Applications. CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H).	8.3	More Details
CVE-2026-12438	Inappropriate implementation in WebView in Google Chrome on Android prior to 149.0.7827.155 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	8.3	More Details
CVE-2026-12437	Use after free in WebShare in Google Chrome on Windows prior to 149.0.7827.155 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	8.3	More Details
CVE-2026-54100	A flaw was found in the Windows Machine Config Operator (WMCO) for Red Hat OpenShift Container Platform. WMCO establishes SSH connections to Windows worker nodes without verifying the remote server host key. An adjacent-network attacker who can intercept or redirect WMCO's SSH session can capture WICD and kubelet bootstrap credentials transferred during node configuration, enabling compromise of Windows node identities in the cluster.	8.3	More Details
CVE-2026-50023	yt-dlp is a command-line audio/video downloader. Prior to 2026.06.09, a vulnerability exists in yt-dlp that allows a remote attacker to write arbitrary OS-shortcut files (such as .desktop, .url, .webloc) to the user's filesystem, bypassing the remediation for CVE-2024-38519. The allowlist explicitly included the unsafe extensions .desktop, .url, and .webloc so that the functionality of the --write-link option (and its variants) could be preserved. These allowlist inclusions can be exploited by an attacker to write malicious OS-shortcut files in the context of a media or subtitles download. This vulnerability is fixed in 2026.06.09.	8.3	More Details
CVE-2026-35302	Vulnerability in the WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in WebLogic Server, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of WebLogic Server. CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).	8.3	More Details
CVE-2025-71337	Flowise before 3.0.10 (affected versions 3.0.7 and earlier) contains an unverified email change vulnerability. An authenticated user can change the account email address, used as a login identifier and password-recovery channel, via the account profile endpoint without confirming the change to the original email address or re-entering the current password. By changing the recovery email, an attacker can take over the account and abuse password reset mechanisms.	8.3	More Details

CVE-2026-54184	Unauthenticated Insecure Direct Object References (IDOR) in Clean Login <= 1.15 versions.	8.2	More Details
CVE-2026-56324	Capgo before 12.128.2 contains a rate limit bypass vulnerability in the channel_self endpoint that allows attackers to circumvent rate limiting by rotating the user-controlled device_id parameter. Attackers can send multiple requests per second by changing device_id values to flood the channel_devices table and cause database exhaustion.	8.2	More Details
CVE-2026-40726	Unauthenticated Broken Access Control in User Registration Stripe <= 1.3.14 versions.	8.2	More Details
CVE-2026-54271	protobufjs-cli is the command line add-on for protobuf.js. Prior to 1.3.2 and 2.5.0, a previous fix for unsafe name handling in pbjs static / static-module code generation was incomplete. Affected versions of protobufjs-cli could still emit unsafe JavaScript references when generating static output from crafted JSON descriptor input. The common case of parsing schemas from .proto files is not affected. This is a bypass of CVE-2026-44295. An attacker who can provide or influence pre-parsed JSON descriptors passed to pbjs static code generation may be able to cause generated JavaScript output to contain attacker-controlled code. The injected code may execute if the generated file is later executed or imported and an affected generated API path is invoked. This vulnerability is fixed in 1.3.2 and 2.5.0.	8.2	More Details
CVE-2026-48109	MessagePack for C# is a MessagePack serializer for C#. Prior to 2.5.301 and 3.1.7, A vulnerability exists in the optional LZ4 decompression path used by MessagePack compression modes Lz4Block and Lz4BlockArray. The decoder implementation is based on a deprecated fast-decompression algorithm that does not take a source-length bound. A remote attacker can send a crafted MessagePack payload with manipulated LZ4 token/length fields to force out-of-bounds reads from the compressed input buffer. In affected environments, this can trigger an AccessViolationException during decompression, causing process termination (denial of service). Under some conditions, limited unintended memory disclosure from over-read data may also be possible before failure. This vulnerability is fixed in 2.5.301 and 3.1.7.	8.2	More Details
CVE-2026-49081	Unauthenticated Broken Access Control in User Registration Stripe <= 1.3.12 versions.	8.2	More Details
CVE-2019-25756	Joomla! Component vAccount 2.0.2 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the vid parameter. Attackers can send GET requests to the vaccount-dashboard/expense endpoint with crafted SQL payloads in the vid parameter to extract sensitive database information including version and database names.	8.2	More Details
CVE-2019-25755	Joomla Component vReview 1.9.11 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the cmId parameter. Attackers can send POST requests to the editReview task endpoint with URL-encoded SQL UNION statements in the cmId parameter to extract database information including usernames, passwords, and database versions.	8.2	More Details
CVE-2026-56785	FlatPress versions prior to commit 10be83c, contains a stored cross-site scripting vulnerability in comment and contact forms where name, URL, and email fields are rendered without proper output encoding in Smarty templates. Attackers can inject arbitrary HTML and JavaScript through these fields to execute malicious scripts in browsers of viewers including administrators, or bypass URL scheme validation to inject javascript: or data: URIs.	8.2	More Details
CVE-2026-56104	Chainlit before 2.10.1 contains a session hijacking vulnerability that allows unauthenticated attackers to restore and inherit authenticated user sessions by presenting a valid sessionId during WebSocket session restoration without ownership verification. Attackers can exploit the restore_existing_session path to assume a victim's permissions and roles, enabling unauthorized invocation of tools and access to data restricted to the authenticated victim.	8.2	More Details
CVE-2017-20252	Joomla NextGen Editor 2.1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL commands through the plname parameter. Attackers can send GET requests to index.php with option=com_nge&view=config and inject malicious SQL code in the plname parameter to extract sensitive database information.	8.2	More Details

CVE-2017-20282	Joomla! Component jCart for OpenCart 2.0 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the product_id parameter. Attackers can send GET requests to index.php with the option=com_jcart&route=product/product parameters and malicious product_id values to extract sensitive database information.	8.2	More Details
CVE-2017-20258	Joomla! Component RPC Responsive Portfolio 1.6.1 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the id parameter. Attackers can send GET requests to index.php with option=com_pofos&view=pofo&id=[SQL] to extract sensitive database information.	8.2	More Details
CVE-2026-46865	Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Extensibility Framework). Supported versions that are affected are 13.5 and 24.1. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Enterprise Manager Base Platform executes to compromise Oracle Enterprise Manager Base Platform. While the vulnerability is in Oracle Enterprise Manager Base Platform, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Manager Base Platform. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	8.2	More Details
CVE-2026-46866	Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Agent Next Gen). Supported versions that are affected are 13.5 and 24.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Enterprise Manager Base Platform. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Enterprise Manager Base Platform as well as unauthorized update, insert or delete access to some of Oracle Enterprise Manager Base Platform accessible data. CVSS 3.1 Base Score 8.2 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H).	8.2	More Details
CVE-2017-20281	Joomla! Component Extra Search 2.2.8 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the establename parameter. Attackers can send GET requests to index.php with the option=com_extrasearch parameter and malicious SQL in the establename field to extract sensitive database information.	8.2	More Details
CVE-2017-20280	Joomla Component Myportfolio 3.0.2 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the pid parameter. Attackers can send GET requests to index.php with malicious pid values in the task=project&view=grid endpoint to extract sensitive database information.	8.2	More Details
CVE-2017-20279	Joomla Payage 2.05 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the aid parameter. Attackers can send GET requests to index.php with malicious aid values in the make_payment task to extract sensitive database information using boolean-based blind or time-based blind techniques.	8.2	More Details
CVE-2017-20278	Joomla Component JoomRecipe 1.0.3 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the category parameter. Attackers can send GET requests to the all-recipes endpoint with malicious SQL payloads in the category path segment to extract sensitive database information.	8.2	More Details
CVE-2017-20277	Joomla JoomRecipe 1.0.4 component contains a blind SQL injection vulnerability in the search_author parameter on the search results page. Attackers can inject SQL code through POST requests to the search endpoint to extract database information using boolean-based blind SQL injection techniques.	8.2	More Details
CVE-2017-20276	Joomla! Component SIMGenealogy 2.1.5 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the type parameter. Attackers can send GET requests to index.php with the option=com_simgenealogy, view=latest parameters and inject malicious SQL in the type parameter to extract sensitive database information.	8.2	More Details
CVE-	Joomla! Component PHP-Bridge 1.2.3 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through		

2017-20275	the id parameter. Attackers can send GET requests to index.php with option=com_phpbridge&view=phpview parameters and inject SQL code in the id parameter to extract database information including table and column names.	8.2	More Details
CVE-2017-20274	Joomla LMS King Professional 3.2.4.0 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the cp_id parameter. Attackers can send GET requests to index.php with the option=com_lmsking, view=lmsking, layout=learningpath, and task=learningPath parameters to extract sensitive database information.	8.2	More Details
CVE-2017-20273	Joomla Event Registration Pro Calendar 4.1.3 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the id parameter. Attackers can send GET requests to index.php with option=com_registrationpro&view=category&id parameter containing SQL injection payloads to extract sensitive database information.	8.2	More Details
CVE-2017-20272	Joomla Ultimate Property Listing 1.0.2 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the sf_selectuser_id parameter. Attackers can send GET requests to index.php with the option=com_upl and view=propertylisting parameters to extract sensitive database information including table names and column structures.	8.2	More Details
CVE-2017-20271	Joomla StreetGuessr Game 1.1.8 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the catid parameter. Attackers can send GET requests to index.php with the option=com_streetguess&view=maps parameters and inject SQL code in the catid parameter to extract sensitive database information including version and database names.	8.2	More Details
CVE-2026-50194	Steeltoe is an open source project that provides a collection of libraries that helps users build cloud-native applications. When Steeltoe management endpoints versions 3.2.2 through 3.3.0 and 4.1.0 are configured to listen on an alternate port (`Management:Endpoints:Port` is configured), the middleware responsible for restricting access to the endpoints uses the `Host` HTTP header rather than the actual network socket port. Versions 3.4.0 and 4.2.0 patch the issue. If an immediate upgrade to a patched version is not possible, add explicit ASP.NET Core authorization (`RequireAuthorization`) to all sensitive actuator endpoints as a defense-in-depth measure independent of port isolation and/or configure the reverse proxy or load balancer to enforce the `Host` header value and prevent clients from setting an arbitrary port.	8.2	More Details
CVE-2017-20270	Joomla! Component Twitch Tv 1.1 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the username and id parameters. Attackers can send GET requests to index.php with option=com_twitchtv and view parameters containing SQL injection payloads to extract sensitive database information including credentials and configuration data.	8.2	More Details
CVE-2017-20269	Joomla! Component KissGallery 1.0.0 contains an SQL injection vulnerability that allows unauthenticated attackers to inject SQL commands through the component URL path. Attackers can supply malicious SQL code in the kissgallery endpoint to execute arbitrary database queries and extract sensitive information.	8.2	More Details
CVE-2017-20268	Joomla! Component Zap Calendar Lite 4.3.4 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the 'eid' parameter. Attackers can send GET requests to the RSVP plugin endpoint with crafted SQL payloads to extract sensitive database information including database names and table structures.	8.2	More Details
CVE-2017-20267	Joomla! Component Calendar Planner 1.0.1 contains an SQL injection vulnerability that allows unauthenticated attackers to inject SQL commands through the category_id parameter. Attackers can send GET requests to the events view with malicious SQL code in the category_id parameter to extract sensitive database information.	8.2	More Details
CVE-2017-20253	Joomla! Component My Projects 2.0 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the VerAyari parameter. Attackers can craft requests to the component endpoint with SQL injection payloads to extract sensitive database information including credentials and system data.	8.2	More Details

CVE-2017-20254	Joomla! Component User Bench 1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the userid parameter. Attackers can send GET requests to index.php with the option=com_userbench&view=detail&userid parameter containing SQL injection payloads to extract sensitive database information including credentials and configuration data.	8.2	More Details
CVE-2017-20255	Joomla! Component JB Visa 1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the visatype parameter. Attackers can send GET requests to index.php with the option=com_bookpro and view=popup parameters, injecting SQL commands in the visatype parameter to extract sensitive database information including credentials and table contents.	8.2	More Details
CVE-2017-20256	Joomla Survey Force Deluxe 3.2.4 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the invite parameter. Attackers can send GET requests to the component with crafted SQL payloads in the invite parameter to extract sensitive database information.	8.2	More Details
CVE-2017-20266	Joomla SP Movie Database 1.3 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the searchword parameter. Attackers can send GET requests to the searchresults view with crafted SQL payloads in the searchword parameter to extract sensitive database information.	8.2	More Details
CVE-2017-20263	Joomla! Component FocalPoint Pro/Free 1.2.3 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the id parameter. Attackers can send GET requests to index.php with option=com_focalpoint, view=location, and a crafted id parameter containing SQL commands to extract sensitive database information.	8.2	More Details
CVE-2017-20257	Joomla! Component Quiz Deluxe 3.7.4 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL commands through the ajaxaction.flag_question task. Attackers can inject malicious SQL code via the stu_quiz_id or flag_quest parameters to manipulate database queries and extract sensitive information.	8.2	More Details
CVE-2017-20262	Joomla! Component Ajax Quiz 1.8 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the cid parameter. Attackers can send GET requests to index.php with the option=com_ajaxquiz and view=ajaxquiz parameters to extract sensitive database information including table names and column structures.	8.2	More Details
CVE-2017-20261	Joomla! Component Bargain Product VM3 1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the product_id parameter. Attackers can supply crafted SQL statements in GET requests to the brainy and alice views to extract sensitive database information.	8.2	More Details
CVE-2017-20260	Joomla! Component Price Alert 3.0.2 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the product_id parameter. Attackers can send requests to the subscribeajax view with crafted SQL payloads in the product_id parameter to extract sensitive database information including credentials and configuration data.	8.2	More Details
CVE-2019-25748	Joomla JHotelReservation 6.0.7 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the rooms parameter. Attackers can send POST requests to the search-hotels endpoint with crafted SQL payloads in the rooms parameter to extract sensitive database information including version details.	8.2	More Details
CVE-2026-55202	Tinyproxy through 1.11.3, fixed in commit 09312a1, fails to properly validate the Host header during stathost detection, allowing unauthenticated attackers to access the stats page by injecting a matching Host header or bypass detection via port manipulation. Remote attackers can trigger unauthorized access to internal proxy statistics or misroute requests as transparent proxy connections to circumvent access controls.	8.2	More Details
CVE-2017-20259	Joomla OSDownloads 1.7.4 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the id parameter. Attackers can send GET requests to index.php with option=com_osdownloads&view=item&id=	8.2	More Details

	[SQL] to extract sensitive database information including credentials and configuration data.		
CVE-2019-25754	Joomla Component vRestaurant 1.9.4 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the keysearch parameter. Attackers can send POST requests to the menu-listing-layout endpoint with crafted SQL payloads in the keysearch parameter to extract database table names and sensitive information from the database.	8.2	More Details
CVE-2026-35288	Vulnerability in the PeopleSoft Enterprise PT PeopleTools product of Oracle PeopleSoft (component: Deployment Package). Supported versions that are affected are 8.61 and 8.62. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where PeopleSoft Enterprise PT PeopleTools executes to compromise PeopleSoft Enterprise PT PeopleTools. While the vulnerability is in PeopleSoft Enterprise PT PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PT PeopleTools. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	8.2	More Details
CVE-2026-35274	Vulnerability in the PeopleSoft Enterprise PT PeopleTools product of Oracle PeopleSoft (component: Deployment Package). Supported versions that are affected are 8.61 and 8.62. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PT PeopleTools. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise PT PeopleTools accessible data as well as unauthorized update, insert or delete access to some of PeopleSoft Enterprise PT PeopleTools accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N).	8.2	More Details
CVE-2019-25752	Joomla! Component J-BusinessDirectory 4.9.7 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the type parameter. Attackers can send GET requests to index.php with the option=com_jbusinessdirectory&task=categories.getCategories parameters and inject UNION-based SQL statements in the type parameter to extract database information including schema names and sensitive data.	8.2	More Details
CVE-2019-25753	Joomla! Component VMap 1.9.6 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code into the latlngbound parameter. Attackers can send GET requests to index.php with the option=com_vmap&task=loadmarker parameters containing SQL injection payloads to manipulate database queries and extract sensitive information.	8.2	More Details
CVE-2019-25751	Joomla Component J-ClassifiedsManager 3.0.5 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through POST parameters. Attackers can submit crafted SQL payloads in the categorySearch, adType, and citySearch parameters to the displayads component to extract sensitive database information including usernames, databases, and version details.	8.2	More Details
CVE-2019-25750	Joomla Component J-MultipleHotelReservation 6.0.7 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the hotel_id parameter. Attackers can send POST requests to the search-hotels endpoint with crafted SQL UNION SELECT statements to extract sensitive database information including table names and column data.	8.2	More Details
CVE-2026-48764	TypeBot is a chatbot builder tool. In versions prior to 3.17.2, SSRF validation is implemented by resolving a hostname once and checking whether the resolved IP belongs to a forbidden range allowing for DNS rebinding bypass. The root cause is a time-of-check to time-of-use gap in the SSRF guard. The validator resolves the hostname and approves it, but the later request path performs a fresh resolution and connects to whatever IP the hostname maps to at that moment. The actual outbound request is then performed later using the original hostname, without pinning the validated IP to the network connection. An attacker who can supply a URL to a public bot that performs a server-side HTTP Request block or server-side script fetch can use DNS rebinding to pass the initial validation and still force the server to connect to a private or metadata address during the real request. This enables server-side access to private network services, cloud metadata endpoints, and other internal HTTP targets that the validator was intended to block. The exact downstream impact depends on the reachable internal services. Concrete consequences include metadata disclosure, access to internal admin panels, credential theft from metadata services, and further compromise through internal-only HTTP interfaces.	8.2	More Details

	This issue has been fixed in version 3.17.2.		
CVE-2026-49260	PhpWeasyPrint is a PHP library allowing PDF generation from a URL or an HTML page. Prior to version 2.5.1, `pontedilana/php-weasyprint` builds the shell command for WeasyPrint by passing the binary path through `escapeshellarg()` first and then checking the *quoted* result with `is_executable()`. On POSIX `escapeshellarg('/usr/local/bin/weasyprint')` returns `'/usr/local/bin/weasyprint'` with the single-quote characters as part of the string, so `is_executable()` looks for a file whose actual name includes those quotes. That file never exists, the "safe" branch is dead code, and the raw `$binary` string (set via the constructor or `setBinary()`) flows directly into `Symfony\Component\Process\Process::fromShellCommandline()`. Any deployment whose binary path is sourced from configuration, an environment variable, or a per-tenant setting reaches a shell-command-injection sink. The library is documented as a one-to-one substitute for KnpLabs/snappy and inherited the exact pre-fix codepath KnpLabs patched in GHSA-vpr4-p6fq-85jc. PhpWeasyPrint version 2.5.1 contains a patch for the issue.	8.2	More Details
CVE-2026-46806	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle WebCenter Content. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebCenter Content accessible data as well as unauthorized update, insert or delete access to some of Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	8.2	More Details
CVE-2026-40739	Unauthenticated PHP Object Injection in LuxeDrive <= 1.4 versions.	8.1	More Details
CVE-2026-41045	A time-to-check-time-of-use in polkit authentication of qSnapper before version 1.3.3 allowed a local attacker to bypass qSnappers authentication mechanism and operate e.g. as root user.	8.1	More Details
CVE-2026-34895	Unauthenticated Local File Inclusion in Softlab Core < 1.2.11 versions.	8.1	More Details
CVE-2026-40736	Unauthenticated PHP Object Injection in Laurits <= 1.5.1 versions.	8.1	More Details
CVE-2026-40735	Unauthenticated PHP Object Injection in Reina <= 2.1 versions.	8.1	More Details
CVE-2026-39443	Unauthenticated PHP Object Injection in EmallShop <= 2.4.21 versions.	8.1	More Details
CVE-2026-39446	Unauthenticated PHP Object Injection in Kapee < 1.7.0 versions.	8.1	More Details
CVE-2026-40731	Unauthenticated Local File Inclusion in ChapterOne <= 1.7 versions.	8.1	More Details
CVE-2026-34894	Unauthenticated Local File Inclusion in Integrio Core < 1.2.8 versions.	8.1	More Details
CVE-2026-	Unauthenticated Local File Inclusion in Thegov Core < 2.0.23 versions.	8.1	More

34893			Details
CVE-2026-56020	The Webmin HTTP server (miniserv.pl) allows unauthenticated attackers to impersonate any user with a configured SSL client certificate by sending a forged HTTP header. A remote attacker can spoof certificate DNs and authenticate as any user. Fixed in 2.641.	8.1	More Details
CVE-2026-39522	Unauthenticated Local File Inclusion in Solene <= 3.4 versions.	8.1	More Details
CVE-2026-39537	Unauthenticated Local File Inclusion in Mikado Core <= 1.6 versions.	8.1	More Details
CVE-2026-42488	Some shadow paging errors paths will switch the page-tables without updating the currently running vCPU reference. This causes a mismatch between the loaded page-tables and the mapcache metadata which can lead to corruption of the mapcache.	8.1	More Details
CVE-2026-49872	Improper Authentication vulnerability in Apache APISIX. When the cas-auth plugin is used in a route, an attacker can possibly authenticate itself with credentials from a different source. This issue affects Apache APISIX: from 3.0.0 through 3.16.0. Users are recommended to upgrade to version 3.17.0, which fixes the issue.	8.1	More Details
CVE-2026-39539	Unauthenticated PHP Object Injection in Alloggio - Hotel Booking <= 2.1.2 versions.	8.1	More Details
CVE-2026-55200	libssh2 through 1.11.1, fixed in commit 7acf3df contains an out-of-bounds write vulnerability in ssh2_transport_read() that fails to enforce upper bounds on packet_length field. Remote attackers can send crafted SSH packets with excessively large packet_length values to corrupt heap memory and achieve remote code execution.	8.1	More Details
CVE-2026-39573	Unauthenticated PHP Object Injection in Mildhill <= 1.5 versions.	8.1	More Details
CVE-2026-47339	Incorrect Authorization vulnerability in Apache APISIX. An attacker can capitalise on authz-casdoor plugin under default configuration to authenticate themselves with credentials from a different source. This issue affects Apache APISIX: from 2.14.1 through 3.16.0. Users are recommended to upgrade to version 3.17.0, which fixes the issue.	8.1	More Details
CVE-2026-56076	PraisonAI before 1.5.128 contains a cross-origin agent execution vulnerability in the AGUI endpoint that allows remote attackers to trigger arbitrary agent execution. The POST /agui endpoint lacks authentication and hardcodes Access-Control-Allow-Origin: * headers, combined with Starlette's Content-Type-agnostic JSON parsing, enabling attackers to bypass CORS preflight checks via simple requests and exfiltrate sensitive agent responses including tool execution results and environment data.	8.1	More Details
CVE-2026-39567	Unauthenticated PHP Object Injection in Santé <= 1.5.1 versions.	8.1	More Details
CVE-2026-39580	Unauthenticated PHP Object Injection in Micdrop <= 1.3.1 versions.	8.1	More Details
CVE-2026-39558	Unauthenticated Local File Inclusion in Malmö <= 2.2 versions.	8.1	More Details
CVE-2026-39582	Unauthenticated Local File Inclusion in Hitek < 1.8.3 versions.	8.1	More Details
CVE-2026-39557	Unauthenticated PHP Object Injection in NeoBeat <= 1.7 versions.	8.1	More Details

CVE-2026-53871	Hermes WebUI before 0.51.368 contains an authorization bypass vulnerability in the get_profile_cookie() function that accepts unauthenticated profile names from the hermes_profile cookie. An authenticated attacker can forge the hermes_profile cookie value to bypass profile-scoped authorization checks and access sessions, files, and resources across different profiles.	8.1	More Details
CVE-2026-39554	Unauthenticated PHP Object Injection in Fidalgo <= 1.2.2 versions.	8.1	More Details
CVE-2026-39549	Unauthenticated Local File Inclusion in Aperitif <= 1.5 versions.	8.1	More Details
CVE-2026-43994	Coturn is a free open source implementation of TURN and STUN Server. Versions prior to 4.10.0 contain a stack buffer overflow in decode_oauth_token_gcm(). A uint16_t nonce_len field read from an attacker-supplied OAuth access token (0-65535) is passed directly to memcpy() as the copy length into a 256-byte stack buffer (oauth_encrypted_block.nonce[256]) without bounds checking. The overflow occurs before AES-GCM authentication is verified, the attacker does not need to know the OAuth key or produce a valid AES-GCM token. Up to 735 bytes of attacker-controlled data are written past the buffer, may corrupt adjacent stack data, including control-flow data depending on compiler, ABI, and mitigations. Requires --oauth mode (non-default). This may provide a plausible RCE primitive depending on exploit mitigations; because coturn is widely deployed for WebRTC TURN/STUN and --oauth is commonly recommended, impact can be broad. This issue has been fixed in version 4.10.0.	8.1	More Details
CVE-2023-45796	A stored cross-site scripting vulnerability in the Runtime component of Pilz PASvisu before 1.14.1 and PMI v8xx up to and including 2.0.33992 allows a low-privileged remote unauthenticated attacker to manipulate process data with potential impact on integrity and/or availability.	8.1	More Details
CVE-2026-39547	Unauthenticated Local File Inclusion in Getaway < 1.8 versions.	8.1	More Details
CVE-2026-39545	Unauthenticated PHP Object Injection in Zermatt <= 1.6.1 versions.	8.1	More Details
CVE-2026-39568	Unauthenticated Local File Inclusion in Mr. SEO <= 2.0 versions.	8.1	More Details
CVE-2026-50107	When NGINX Plus or NGINX Open Source is configured as the data plane for NGINX Gateway Fabric, an injection vulnerability exists in the NGINX configuration generator component of NGINX Gateway Fabric. User-supplied string values from the NginxProxy Custom Resource Definition (CRD) access log format setting are rendered directly into NGINX configuration templates without sanitization or escaping. An authenticated attacker with permission to create or modify these CRDs may craft values that inject arbitrary NGINX configuration directives. This is a control plane issue; there is no data plane exposure from the vulnerability trigger itself. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	8.1	More Details
CVE-2026-40756	Unauthenticated PHP Object Injection in Zoya <= 1.4 versions.	8.1	More Details
CVE-2026-40751	Unauthenticated PHP Object Injection in Ashtanga <= 1.2 versions.	8.1	More Details
CVE-2026-32804	Dell PowerFlex Manager, version(s) [Versions], contain(s) an Improper Authentication vulnerability. An unauthenticated attacker with adjacent network access could potentially exploit this vulnerability, leading to Unauthorized access.	8.1	More Details
	When NGINX Plus is configured as the data plane for NGINX Gateway Fabric, an injection vulnerability exists in the NGINX configuration generator component of NGINX Gateway Fabric.		

CVE-2026-11311	User-supplied string values from the NginxProxy Custom Resource Definition serverTokens field and the AuthenticationFilter Custom Resource Definition extraAuthArgs field are rendered directly into NGINX configuration templates without sanitization or escaping. An authenticated attacker with permission to create or modify these Custom Resource Definitions may craft values that inject arbitrary NGINX configuration directives. This is a control plane issue; there is no data plane exposure from the vulnerability trigger itself. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	8.1	More Details
CVE-2025-69157	Unauthenticated Local File Inclusion in Gamic <= 1.15 versions.	8.1	More Details
CVE-2025-69158	Unauthenticated Local File Inclusion in Granola <= 1.13 versions.	8.1	More Details
CVE-2025-69164	Unauthenticated Local File Inclusion in Skyward <= 1.10 versions.	8.1	More Details
CVE-2025-69166	Unauthenticated Local File Inclusion in Gunslinger <= 1.7 versions.	8.1	More Details
CVE-2025-69170	Unauthenticated Local File Inclusion in Eventicity <= 1.5 versions.	8.1	More Details
CVE-2025-69174	Unauthenticated Local File Inclusion in Etude <= 1.6 versions.	8.1	More Details
CVE-2025-69175	Unauthenticated Local File Inclusion in Line Agency <= 1.3.1 versions.	8.1	More Details
CVE-2026-54814	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in StylemixThemes Motors allows PHP Local File Inclusion. This issue affects Motors: from n/a through 1.4.109.	8.1	More Details
CVE-2026-39442	Unauthenticated PHP Object Injection in PressMart <= 1.2.26 versions.	8.1	More Details
CVE-2026-39445	Unauthenticated PHP Object Injection in Alukas < 3.0.0 versions.	8.1	More Details
CVE-2026-39523	Unauthenticated Local File Inclusion in Solene Core <= 2.3.2 versions.	8.1	More Details
CVE-2026-39556	Unauthenticated PHP Object Injection in Konsept <= 1.9 versions.	8.1	More Details
CVE-2026-39559	Unauthenticated Local File Inclusion in Uppercase < 1.2.2 versions.	8.1	More Details
CVE-2026-39560	Unauthenticated PHP Object Injection in Hiroshi <= 1.5.1 versions.	8.1	More Details
CVE-2026-	Unauthenticated PHP Object Injection in SingleMalt <= 1.5 versions.	8.1	More Details

39576			
CVE-2026-39590	Unauthenticated Local File Inclusion in Atomlab <= 2.4.5 versions.	8.1	More Details
CVE-2026-40733	Unauthenticated PHP Object Injection in ShiftUp <= 1.3 versions.	8.1	More Details
CVE-2026-40738	Unauthenticated PHP Object Injection in Eldon <= 1.4.1 versions.	8.1	More Details
CVE-2026-40752	Unauthenticated PHP Object Injection in Manufaktur Solutions <= 1.1.1 versions.	8.1	More Details
CVE-2026-52707	Unauthenticated Local File Inclusion in Kastell <= 2.0 versions.	8.1	More Details
CVE-2025-69144	Unauthenticated Local File Inclusion in Preservation <= 1.10 versions.	8.1	More Details
CVE-2025-69126	Unauthenticated Local File Inclusion in Fortius <= 2.3.0 versions.	8.1	More Details
CVE-2026-40753	Unauthenticated PHP Object Injection in EasyMeals <= 1.5.1 versions.	8.1	More Details
CVE-2025-69123	Unauthenticated Local File Inclusion in Snow Club <= 1.1 versions.	8.1	More Details
CVE-2026-40754	Unauthenticated PHP Object Injection in Roisin <= 1.4 versions.	8.1	More Details
CVE-2026-40755	Unauthenticated PHP Object Injection in TechLink <= 1.3 versions.	8.1	More Details
CVE-2026-40758	Unauthenticated PHP Object Injection in Léonie <= 1.2.1 versions.	8.1	More Details
CVE-2026-40759	Unauthenticated PHP Object Injection in Esmée <= 1.4 versions.	8.1	More Details
CVE-2026-40760	Unauthenticated PHP Object Injection in Behold <= 1.5 versions.	8.1	More Details
CVE-2026-40761	Unauthenticated PHP Object Injection in Valeska <= 1.2.2 versions.	8.1	More Details
CVE-2026-40757	Unauthenticated PHP Object Injection in Château <= 1.2.1 versions.	8.1	More Details
CVE-2025-	picklescan before 0.0.30 fails to detect cProfile.runctx function calls in pickle file reduce methods, allowing attackers to execute arbitrary code. Malicious pickle files bypass picklescan	8.1	More

71378	detection and execute remote code when loaded via pickle.load().		Details
CVE-2025-71357	picklescan before 0.0.30 fails to detect malicious pickle files using idlelib.pyshell.ModifiedInterpreter.runcommand in reduce methods. Attackers can embed undetected code in pickle files that executes remote commands when loaded by victims.	8.1	More Details
CVE-2025-71348	picklescan before 0.0.28 fails to detect malicious pickle files that invoke torch.utils._config_module.load_config function within reduce methods. Attackers can craft pickle files embedding arbitrary code that evades detection but executes during pickle.load, enabling remote code execution in supply chain attacks.	8.1	More Details
CVE-2026-56345	AVideo through 29.0 contains an authorization bypass vulnerability in the Meet plugin's uploadRecordedVideo.json.php endpoint that derives the target users_id from the uploaded filename without verification. An attacker with knowledge of the Meet shared secret can craft a malicious file upload with a filename containing an arbitrary users_id to invoke passwordless User->login() and establish an authenticated session as any user including admin. Attackers can obtain the Meet shared secret through path-traversal vulnerabilities or timing attacks against checkToken.json.php, then POST a crafted file to uploadRecordedVideo.json.php with a filename like '1-anything.mp4' to hijack admin sessions and gain full account takeover.	8.1	More Details
CVE-2026-54415	Missing Authorization in the server management routes (routes/admin.php) in Azuriom Azuriom CMS before 1.2.11 on all platforms allows an authenticated attacker with the admin.access permission to create AzLink server tokens and take over non-admin user accounts by changing their passwords and email addresses via crafted HTTP requests to /admin/servers/create and the AzLink API endpoints (/api/azlink/password, /api/azlink/email, /api/azlink/user/{id}).	8.1	More Details
CVE-2026-9843	The Database for Contact Form 7, WPforms, Elementor forms plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the view_page function in all versions up to, and including, 1.5.1. This makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php). Successful exploitation requires an administrator to view or edit the poisoned form entry, at which point PHP's bracket parser reshapes the attacker-crafted JSON key to bypass the stored-path isset check and trigger deletion of the traversal-specified file.	8.1	More Details
CVE-2026-42530	NGINX Open Source has a vulnerability in the ngx_http_v3_module module. When NGINX Open Source is configured to use the HTTP/3 QUIC module, a remote unauthenticated attacker along with conditions beyond their control can use a specially crafted HTTP/3 session to reopen a QPACK encoder stream. This may cause a Use-after-Free in the NGINX worker process leading to a restart. Additionally, attackers can execute code on systems with Address Space Layout Randomization (ASLR) disabled or when the attacker can bypass ASLR. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	8.1	More Details
CVE-2026-42055	NGINX Plus and NGINX Open Source have a vulnerability in the ngx_http_proxy_v2_module and ngx_http_grpc_module modules. This vulnerability exists when the proxy_http_version to 2 or grpc_pass directives are used to proxy HTTP/2 traffic, the ignore_invalid_headers directive is set to off, and the large_client_header_buffers directive size is larger than 2 megabytes. A remote, unauthenticated attacker, along with conditions beyond their control, could send large headers while creating an upstream request. This may cause a heap-based buffer overflow in the NGINX worker process leading to a restart. Additionally, attackers can execute code on systems with Address Space Layout Randomization (ASLR) disabled or when the attacker can bypass ASLR. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	8.1	More Details
CVE-2026-49340	gonic is a music streaming server / free-software subsonic server API implementation. Prior to version 0.21.0, a logic error in `ServeCreateOrUpdatePlaylist` allows any authenticated Subsonic user (including non-admin) to write playlist M3U content to an attacker-controlled absolute filesystem path on the gonic host, and to create intermediate directories with `0o777` permissions. The bug is independent of CVE-2026-49338 and CVE-2026-49339. It is an unreachable guard clause combined with no path containment in `Store.Write`. Version 0.21.0 patches the issue.	8.1	More Details
CVE-2026-	mcp-memory-service is a semantic memory layer for AI applications. Prior to version 10.65.3, the HTTP MCP JSON-RPC endpoint at `/mcp` requires only OAuth `read` scope for all requests, then dispatches `tools/call` directly to handlers that include mutating tools. A read-only OAuth	8.1	More Details

49291	client can call `store_memory` and `delete_memory` through MCP even though the corresponding REST endpoints require `write` scope. Version 10.65.3 patches the issue.		
CVE-2026-49286	PhpWeasyPrint is a PHP library allowing PDF generation from a URL or an HTML page. Prior to version 2.6.0, `pontedilana/php-weasyprint` guarded the output filename against the `phar://` stream wrapper with a case-sensitive blacklist. PHP stream wrappers are case-insensitive, so `PHAR://`, `Phar://`, etc. bypass the check and reach `fileExists()` (`file_exists()`) in `prepareOutput()`. On PHP 7 (which the library still supports — PHP 7.4+), this triggers deserialization of a crafted PHAR archive's metadata, leading to remote code execution. This is the patch-bypass of CVE-2023-28115. The same issue and fix were handled upstream in KnpLabs/snappy (GHSA-92rv-4j2h-8mjj). PhpWeasyPrint version 2.6.0 contains a patch for the issue.	8.1	More Details
CVE-2025-69106	Unauthenticated Local File Inclusion in Imba <= 1.5.0 versions.	8.1	More Details
CVE-2025-69115	Unauthenticated Local File Inclusion in LuxMed | Medicine & Healthcare Doctor WordPress Theme <= 1.2.2 versions.	8.1	More Details
CVE-2025-69120	Unauthenticated Local File Inclusion in Dazzle <= 1.0.0 versions.	8.1	More Details
CVE-2025-66336	Apache Doris MCP Server contains a SQL injection vulnerability in a metadata query path. A user-controlled database name is directly interpolated into a SQL query, and the query is executed without passing the caller's authorization context. This may allow an authenticated attacker, or an anonymous attacker if authentication is disabled, to bypass SQL security validation and access metadata outside the intended database scope. Affected users are recommended to upgrade to Doris version 0.6.1 or later, which fixes the issue.	8.1	More Details
CVE-2026-55744	Cotonti 1.0.0 (master branch, commit f43f1fc3) is vulnerable to Cross-Site Request Forgery in the Personal File Storage (PFS) module. In modules/pfs/inc/pfs.main.php, the file upload action ('a=upload') processes uploaded files without calling cot_check_xg() to validate the anti-CSRF token, even though sibling actions such as 'delete' (line 272) do. A remote attacker who lures an authenticated user into visiting a malicious page can force the browser to submit a forged multipart request that uploads arbitrary files into the victim's PFS storage.	8.1	More Details
CVE-2025-69162	Unauthenticated Local File Inclusion in Grecko <= 5.17 versions.	8.1	More Details
CVE-2025-69178	Unauthenticated Local File Inclusion in Truemag <= 4.3.14.2 versions.	8.1	More Details
CVE-2025-69121	Unauthenticated Local File Inclusion in Deliciosa <= 1.10.0 versions.	8.1	More Details
CVE-2025-69124	Unauthenticated Local File Inclusion in Especio <= 1.0 versions.	8.1	More Details
CVE-2025-69125	Unauthenticated Local File Inclusion in Food Drop <= 1.3 versions.	8.1	More Details
CVE-2025-69136	Unauthenticated Local File Inclusion in Wanium <= 1.9.8 versions.	8.1	More Details
CVE-2025-69141	Unauthenticated Local File Inclusion in Kelly Young <= 1.1.0 versions.	8.1	More Details

CVE-2025-69142	Unauthenticated Local File Inclusion in Abelle <= 1.22 versions.	8.1	More Details
CVE-2025-69143	Unauthenticated Local File Inclusion in Mission <= 1.22 versions.	8.1	More Details
CVE-2025-69145	Unauthenticated Local File Inclusion in Gat <= 1.16 versions.	8.1	More Details
CVE-2025-69146	Unauthenticated Local File Inclusion in Dom <= 1.24 versions.	8.1	More Details
CVE-2025-69147	Unauthenticated Local File Inclusion in Putter <= 1.17 versions.	8.1	More Details
CVE-2025-69148	Unauthenticated Local File Inclusion in Quirky <= 1.23 versions.	8.1	More Details
CVE-2025-69149	Unauthenticated Local File Inclusion in Top Dog <= 1.0.5 versions.	8.1	More Details
CVE-2025-69150	Unauthenticated Local File Inclusion in Medeus <= 1.14 versions.	8.1	More Details
CVE-2025-69159	Unauthenticated Local File Inclusion in Printo <= 1.11 versions.	8.1	More Details
CVE-2025-69160	Unauthenticated Local File Inclusion in Gita <= 1.11 versions.	8.1	More Details
CVE-2025-69161	Unauthenticated Local File Inclusion in Snowy <= 1.13 versions.	8.1	More Details
CVE-2026-46851	Vulnerability in the PeopleSoft Enterprise CS Campus Community product of Oracle PeopleSoft (component: Security). The supported version that is affected is 9.2.38. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise CS Campus Community. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise CS Campus Community. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	8.1	More Details
CVE-2026-46920	Vulnerability in the Siebel CRM Cloud Applications product of Oracle Siebel CRM (component: Siebel Cloud Manager). Supported versions that are affected are 17.0-26.5. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel CRM Cloud Applications. Successful attacks of this vulnerability can result in takeover of Siebel CRM Cloud Applications. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	8.1	More Details
CVE-2025-69163	Unauthenticated Local File Inclusion in WineShop <= 3.17 versions.	8.1	More Details
CVE-2025-69165	Unauthenticated Local File Inclusion in Choreo <= 1.6 versions.	8.1	More Details

CVE-2025-69167	Unauthenticated Local File Inclusion in Eros <= 1.3 versions.	8.1	More Details
CVE-2025-69168	Unauthenticated Local File Inclusion in Spike <= 1.2 versions.	8.1	More Details
CVE-2025-69171	Unauthenticated Local File Inclusion in Orpheus <= 1.3 versions.	8.1	More Details
CVE-2025-69172	Unauthenticated Local File Inclusion in Resurs <= 1.3 versions.	8.1	More Details
CVE-2025-69173	Unauthenticated Local File Inclusion in Tipsy <= 1.1 versions.	8.1	More Details
CVE-2026-46849	Vulnerability in the PeopleSoft Enterprise CS Student Financials product of Oracle PeopleSoft (component: Other). The supported version that is affected is 9.2.38. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise CS Student Financials. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all PeopleSoft Enterprise CS Student Financials accessible data as well as unauthorized access to critical data or complete access to all PeopleSoft Enterprise CS Student Financials accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2025-69176	Unauthenticated Local File Inclusion in ITactics <= 1.0 versions.	8.1	More Details
CVE-2025-69119	Unauthenticated Local File Inclusion in Corbesier <= 1.15.0 versions.	8.1	More Details
CVE-2025-69118	Unauthenticated Local File Inclusion in CopyPress <= 1.4.5 versions.	8.1	More Details
CVE-2025-69117	Unauthenticated Local File Inclusion in Ingenioso <= 1.14.0 versions.	8.1	More Details
CVE-2025-71365	picklescan before 0.0.33 fails to detect malicious pickle files that invoke numpy.f2py.crackfortran.myeval function through the reduce method. Attackers can craft malicious pickle files embedding arbitrary code that evades picklescan detection and executes remote code when loaded.	8.1	More Details
CVE-2026-46898	Vulnerability in the Oracle Enterprise Command Center Framework product of Oracle E-Business Suite (component: Core). Supported versions that are affected are V15 and V16. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Enterprise Command Center Framework. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Enterprise Command Center Framework accessible data as well as unauthorized access to critical data or complete access to all Oracle Enterprise Command Center Framework accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-	Vulnerability in the Oracle Configure to Order product of Oracle E-Business Suite (component: Supply to Order Workbench). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Configure to Order. Successful attacks of this vulnerability can result in		More

2026-46939	unauthorized creation, deletion or modification access to critical data or all Oracle Configure to Order accessible data as well as unauthorized access to critical data or complete access to all Oracle Configure to Order accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	Details
CVE-2026-46891	Vulnerability in the JD Edwards EnterpriseOne Accounts Payable product of Oracle JD Edwards (component: Accounts Payable). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Accounts Payable. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all JD Edwards EnterpriseOne Accounts Payable accessible data as well as unauthorized access to critical data or complete access to all JD Edwards EnterpriseOne Accounts Payable accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2026-45135	Caddy is an extensible server platform that uses TLS by default. From 2.7.0 until 2.11.3, the FastCGI transport's splitPos() in modules/caddyhttp/reverseproxy/fastcgi/fastcgi.go misuses golang.org/x/text/search with search.IgnoreCase when the request path contains a non-ASCII byte. Two distinct flaws in that fallback let an attacker mislead Caddy's FastCGI splitting into treating a non-.php (or other configured split_path extension) file as a script. In any deployment where the attacker can place content into a file served via FastCGI (uploads, file storage, etc.), this can be escalated to remote code execution by crafting a URL whose path triggers either flaw. This vulnerability is fixed in 2.11.3.	8.1	More Details
CVE-2026-49402	Deno is a JavaScript, TypeScript, and WebAssembly runtime. Prior to 2.7.10, Deno's node:child_process implementation provided an escapeShellArg() helper used when callers passed shell: true to spawn / spawnSync / exec and friends. On Windows, the helper failed to quote arguments that contained cmd.exe metacharacters and did not neutralize % (which cmd.exe expands even inside double-quoted strings). An attacker who controlled any portion of an argument passed to such a call could inject arbitrary additional commands into the spawned cmd.exe invocation. This vulnerability is fixed in 2.7.10.	8.1	More Details
CVE-2026-35019	NetComm NF20MESH routers running firmware R6B031 and earlier contain an authentication bypass vulnerability that allows unauthenticated attackers to gain administrative access by exploiting a hardcoded AES-256 key used to encrypt session cookies for the web management interface. Attackers can forge a valid encrypted session cookie using the shared hardcoded key and bypass authentication checks to obtain full administrative control of the management interface while any legitimate administrator session is active.	8.1	More Details
CVE-2026-56784	OpenRemote before 1.25.0 contains an insecure direct object reference (IDOR) vulnerability in the bulk alarm deletion endpoint that allows authenticated users to permanently delete alarms belonging to other tenants by supplying arbitrary alarm IDs. The removeAlarms() method in AlarmResourceImpl.java omits realm-scoping validation in its JPA query, enabling any user with alarm-write permissions to enumerate sequential auto-increment alarm IDs and delete cross-tenant alarm records without authorization.	8.1	More Details
CVE-2026-56258	Crawl4AI before 0.8.8 contains an arbitrary file write vulnerability in the screenshot and PDF endpoints that allows unauthenticated attackers to write files outside the intended directory via symlink and time-of-check-time-of-use (TOCTOU) attacks on the output_path parameter. Remote attackers can exploit insufficient path validation and symlink following to achieve arbitrary file write and potential code execution on systems where the runtime user has write access to executable or cron locations.	8.1	More Details
CVE-2026-52845	Caddy is an extensible server platform that uses TLS by default. Prior to 2.11.4, forward_auth copy_headers deletes the exact client-supplied identity header before copying the trusted value from the auth gateway. But when the request later goes through php_fastcgi, Caddy normalizes HTTP headers into CGI variables by replacing - with _. This lets a client send an underscore alias that survives the forward_auth delete step but becomes the same PHP/FastCGI variable. Result: a remote client can inject or sometimes override identity/group headers trusted by PHP/FastCGI applications behind Caddy. This vulnerability is fixed in 2.11.4.	8.1	More Details
CVE-2026-56243	Capgo before 12.128.2 contains a security control bypass vulnerability where the PostgREST/RLS plane accepts plaintext API keys through the capgkey header despite enforce_hashed_api_keys being enabled. Attackers can bypass org-level hashed-key enforcement by sending plaintext API keys directly to the PostgREST/RLS plane to access protected resources.	8.1	More Details

CVE-2025-71376	picklescan before 0.0.29 fails to detect malicious pickle files using idlelib.autocomplete.AutoComplete.fetch_completions in reduce methods. Attackers can embed undetected code in pickle files that executes arbitrary commands when loaded by victims.	8.1	More Details
CVE-2025-71370	picklescan before 0.0.28 fails to detect malicious torch.jit.unsupported_tensor_ops.execWrapper function calls embedded in pickle files. Attackers can craft malicious pickle files that bypass picklescan detection and execute arbitrary code when loaded via pickle.load().	8.1	More Details
CVE-2025-58924	Unauthenticated Local File Inclusion in Geya <= 1.15 versions.	8.1	More Details
CVE-2025-69116	Unauthenticated Local File Inclusion in Iona <= 1.0.8 versions.	8.1	More Details
CVE-2025-58952	Unauthenticated Local File Inclusion in Neuronet < 1.14.0 versions.	8.1	More Details
CVE-2025-58953	Unauthenticated Local File Inclusion in Joly <= 1.22.0 versions.	8.1	More Details
CVE-2025-58954	Unauthenticated Local File Inclusion in HomeRoofer <= 2.11.0 versions.	8.1	More Details
CVE-2025-71341	picklescan before 0.0.29 fails to detect the profile.Profile.runctx function when analyzing pickle files, allowing attackers to embed undetected malicious code. Remote attackers can craft malicious pickle files using profile.Profile.runctx in the reduce method to achieve remote code execution when the pickle file is loaded.	8.1	More Details
CVE-2025-60085	Unauthenticated Local File Inclusion in Learnify <= 1.15.0 versions.	8.1	More Details
CVE-2025-69105	Unauthenticated Local File Inclusion in Modernee <= 1.6.0 versions.	8.1	More Details
CVE-2025-69107	Unauthenticated Local File Inclusion in Rosaleen <= 2.8 versions.	8.1	More Details
CVE-2025-69109	Unauthenticated Local File Inclusion in Raider Spirit <= 1.1.2 versions.	8.1	More Details
CVE-2025-69110	Unauthenticated Local File Inclusion in AirSupply <= 2.0.0 versions.	8.1	More Details
CVE-2025-69112	Unauthenticated Local File Inclusion in Planty <= 1.14.0 versions.	8.1	More Details
CVE-2025-69113	Unauthenticated Local File Inclusion in Nexio <= 1.10.0 versions.	8.1	More Details
CVE-2025-69114	Unauthenticated Local File Inclusion in MaxiNet <= 1.2.10 versions.	8.1	More Details
CVE-			More

2025-69177	Unauthenticated Local File Inclusion in Roneous <= 2.1.5 versions.	8.1	Details
CVE-2026-46927	Vulnerability in the Oracle Receivables product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows unauthenticated attacker with network access via SOAP to compromise Oracle Receivables. Successful attacks of this vulnerability can result in takeover of Oracle Receivables. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	8.1	More Details
CVE-2026-35279	Vulnerability in the PeopleSoft Enterprise PT PeopleTools product of Oracle PeopleSoft (component: Performance Monitor). Supported versions that are affected are 8.61 and 8.62. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PT PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PT PeopleTools. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	8.1	More Details
CVE-2026-25439	Unauthenticated Broken Authentication in Booknetic <= 4.8.5 versions.	8.1	More Details
CVE-2026-22338	Unauthenticated Local File Inclusion in EcoBlue <= 1.15 versions.	8.1	More Details
CVE-2026-35289	Vulnerability in the PeopleSoft Enterprise PT PeopleTools product of Oracle PeopleSoft (component: Deployment Package). Supported versions that are affected are 8.61 and 8.62. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise PeopleSoft Enterprise PT PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PT PeopleTools. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	8.1	More Details
CVE-2026-22331	Unauthenticated Local File Inclusion in AutoParts <= 1.5.8 versions.	8.1	More Details
CVE-2026-22330	Unauthenticated Local File Inclusion in Right Way <= 4.0 versions.	8.1	More Details
CVE-2026-55388	piscina is a node.js worker pool implementation. Prior to 6.0.0-rc.2, 5.2.0, and 4.9.3, piscina's constructor and run() paths read the filename option via plain member access. Both reads fall through the prototype chain when the caller's options object doesn't have filename as an own property. When Object.prototype.filename is polluted upstream the inherited value flows to worker_threads.Worker import and the attacker's .mjs runs in the worker. This vulnerability is fixed in 6.0.0-rc.2, 5.2.0, and 4.9.3.	8.1	More Details
CVE-2026-54512	jackson-databind contains the general-purpose data-binding functionality and tree-model for Jackson Data Processor. From 2.10.0 until 2.18.8, 2.21.4, and 3.1.4, jackson-databind's PolymorphicTypeValidator (PTV) is the primary safety mechanism guarding polymorphic deserialization. When polymorphic typing is enabled and a type identifier contains generic parameters (i.e. the type ID string contains <), DatabindContext._resolveAndValidateGeneric() validates only the raw container class name (the substring before <) against the configured PTV. If the container type is approved, the method parses the full canonical type string via TypeFactory.constructFromCanonical() and returns the fully parameterized type without ever validating the nested type arguments against the PTV. The nested type arguments are then resolved, instantiated, and populated as beans during deserialization. An attacker who controls the type ID can therefore place a denied class as a generic type parameter of an allowed container — for example java.util.ArrayList<com.evil.Gadget> when only java.util.ArrayList is allow-listed. The container passes the PTV check; com.evil.Gadget is loaded via Class.forName(name, true, loader), instantiated, and its properties are set from attacker-controlled JSON. This completely bypasses an explicitly configured PTV allow-list. This vulnerability is fixed in 2.18.8, 2.21.4, and 3.1.4.	8.1	More Details

CVE-2026-22326	Unauthenticated Local File Inclusion in Reprizo <= 1.0.8 versions.	8.1	More Details
CVE-2026-22325	Unauthenticated Local File Inclusion in Promo <= 1.3.0 versions.	8.1	More Details
CVE-2026-44271	Dell Wyse Management Suite (WMS), versions prior to WMS 2605, contain an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Unauthorized access.	8.1	More Details
CVE-2026-9072	IBM i 7.6, 7.5, 7.4, and 7.3, IBM WebSphere Application Server, and IBM WebSphere Application Server Liberty - when using Intelligent Management with the WebSphere WebServer Plug-in component - are vulnerable to remote code execution and denial of service. This vulnerability can be exploited when an attacker impersonates backend servers and sends crafted responses to the plug-in.	8.1	More Details
CVE-2026-39253	An issue in Pivotal CRM v.6.6.04.08 allows a remote attacker to execute arbitrary code via the Pivotal.Core.Common.dll and Pivotal.Engine.Client.Services.Conversion.dll components.	8.1	More Details
CVE-2026-54513	jackson-databind contains the general-purpose data-binding functionality and tree-model for Jackson Data Processor. From 2.10.0 until 2.18.8, 2.21.4, and 3.1.4, BasicPolymorphicTypeValidator.Builder.allowIfSubTypeIsArray() allowlists any array type based only on clazz.isArray(), without validating the array's component (element) type against the configured allowlist. A PTV built with allowIfSubTypeIsArray() plus an explicit concrete-type allowlist therefore still permits EvilType[] even though EvilType is not allowlisted. When Jackson deserializes the elements and no per-element type IDs are present, it instantiates the component type directly with no further PTV check, bypassing the allowlist. This vulnerability is fixed in 2.18.8, 2.21.4, and 3.1.4.	8.1	More Details
CVE-2025-71339	Picklescan before 0.0.33 fails to detect the numpy.f2py.crackfortran._eval_length gadget in pickle __reduce__ methods, allowing arbitrary code execution. Attackers can craft malicious pickle files that execute arbitrary Python code when loaded by victims who trust Picklescan's safety validation.	8.1	More Details
CVE-2025-71344	picklescan before 0.0.30 (affected versions 0.0.26 and earlier) fails to detect the ensurepip._run_pip built-in function when scanning pickle files, allowing attackers to execute arbitrary code. Malicious pickle files embedding ensurepip._run_pip calls in __reduce__ methods bypass picklescan detection and achieve remote code execution upon pickle.load() invocation.	8.1	More Details
CVE-2025-71358	picklescan before 0.0.29 fails to detect malicious pickle files that exploit idlelib.autocomplete.AutoComplete.get_entity function in reduce methods. Attackers can embed undetected code in pickle files that executes arbitrary commands when loaded by victims using pickle.load().	8.1	More Details
CVE-2026-35276	Vulnerability in the PeopleSoft Enterprise PT PeopleTools product of Oracle PeopleSoft (component: Application Server). Supported versions that are affected are 8.61 and 8.62. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PT PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PT PeopleTools. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	8.1	More Details
CVE-2026-46787	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). The supported version that is affected is 14.1.2.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Content accessible data as well as unauthorized access to critical data or complete access to all Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 8.0 (Confidentiality and Integrity impacts). CVSS Vector:	8.0	More Details

	(CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:N).		
CVE-2026-46796	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Sites. CVSS 3.1 Base Score 8.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H).	8.0	More Details
CVE-2025-48640	In multiple locations, there is a possible 3rd party passkey entry pairing approval due to a missing permission check. This could lead to remote (proximal/adjacent) escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.0	More Details
CVE-2026-39598	Unrestricted Upload of File with Dangerous Type vulnerability in Kodezen LLC Academy LMS Pro allows Upload a Web Shell to a Web Server. This issue affects Academy LMS Pro: from n/a before 3.5.2.	8.0	More Details
CVE-2026-46894	Vulnerability in the Oracle iSupplier Portal product of Oracle E-Business Suite (component: Home Page). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise Oracle iSupplier Portal. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle iSupplier Portal. CVSS 3.1 Base Score 8.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H).	8.0	More Details
CVE-2026-42487	HVM guest I/O port accesses are subject to either emulation or at least translation. Translations are managed by the device model (via XEN_DOMCTL_ioport_mapping), and hence the linked list used may changed at any time. Traversal of those lists (while handling guest I/O port accesses) therefore needs synchronizing with updates, which was missing so far.	7.9	More Details
CVE-2026-46848	Vulnerability in the WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 14.1.2.0.0 and 15.1.1.0.0. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where WebLogic Server executes to compromise WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in WebLogic Server, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all WebLogic Server accessible data as well as unauthorized access to critical data or complete access to all WebLogic Server accessible data. CVSS 3.1 Base Score 7.9 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:N).	7.9	More Details
CVE-2016-20095	Matrix42 Remote Control Host 3.20.0031 contains an unquoted service path vulnerability in the FastViewerRemoteService and FastViewerRemoteProxy services that allows local users to execute arbitrary code with SYSTEM privileges. Attackers can place a malicious executable in the Program Files directory with a crafted name to be executed by the service during startup, gaining elevated privileges.	7.8	More Details
CVE-2026-12958	Missing symlink validation in Language Servers for AWS may allow an arbitrary file write outside of the workspace trust boundary. This may occur when a local user opens a workspace with a maliciously crafted symlink that resolves to a file path outside the workspace trust boundary. To remediate this issue, users should upgrade to version 1.69.0 or higher.	7.8	More Details
CVE-2020-9695	Acrobat Reader versions 2020.009.20074, 2020.001.30002, 2017.011.30171, 2015.006.30523 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-2026-12784	A weakness has been identified in IM-Magic Partition Resizer up to 7.9.0. This affects an unknown function in the library MDA_NTDRV.sys of the component Kernel Driver. This manipulation causes improper access controls. The attack requires local access. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	7.8	More Details

CVE-2026-46888	Vulnerability in the Siebel CRM Deployment product of Oracle Siebel CRM (component: Database Upgrade). Supported versions that are affected are 17.0-26.5. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Siebel CRM Deployment executes to compromise Siebel CRM Deployment. Successful attacks of this vulnerability can result in takeover of Siebel CRM Deployment. CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	7.8	More Details
CVE-2026-32652	Dell AIOps Collector versions prior to 1.18.3 contain a "Use of Default Credentials" vulnerability. A low privileged attacker with console access could potentially exploit this vulnerability to gain Filesystem access. This vulnerability only affects fresh installations of Collector versions earlier than 1.18.3. Systems that have been upgraded (either manually or automatically) to version 1.18.3 or later are not impacted, even if they were originally installed on an earlier version.	7.8	More Details
CVE-2025-71326	AVAST Antivirus 25.11 contains an unquoted service path vulnerability in the SecureLine service that allows local non-privileged users to execute code with elevated SYSTEM privileges. Attackers can exploit the unquoted binary path in the service configuration to inject malicious executables that execute with high-level system permissions.	7.8	More Details
CVE-2016-20090	Comodo Dragon Browser versions up to 52.15.25.663 contain a privilege escalation vulnerability in the DragonUpdater service due to an unquoted service path running with SYSTEM privileges. A local attacker can insert a malicious executable in the service path and execute arbitrary code with elevated privileges upon service restart or system reboot.	7.8	More Details
CVE-2016-20091	Windows Firewall Control 4.8.6.0 contains an unquoted service path vulnerability that allows local attackers to escalate privileges by inserting malicious executables in the service path. Attackers can place executable files in unquoted path directories that the wfcs.exe service will execute with LocalSystem privileges upon service restart or system reboot.	7.8	More Details
CVE-2023-54353	Chromacam 4.0.3.0 contains an unquoted service path vulnerability in the PsyFrameGrabberService that allows local attackers to execute arbitrary code by placing malicious executables in unquoted path directories. Attackers with write access to C:\ or subdirectories like C:\Program Files (x86)\Personify\ can place a malicious Program.exe or PsyFrameGrabberService.exe file that executes with LocalSystem privileges when the service starts automatically at boot.	7.8	More Details
CVE-2022-50971	Malwarebytes 4.5 contains an unquoted service path vulnerability in the MBAMService executable that allows local attackers to escalate privileges by injecting malicious code into the system root path. Attackers can place executable files in unquoted path directories that execute with LocalSystem privileges during service startup or system reboot.	7.8	More Details
CVE-2021-47985	Brother SAPSprint 7.60 contains an unquoted service path vulnerability in the SAPSprint service binary that allows local attackers to escalate privileges. Attackers can place a malicious executable in the Program Files directory path to be executed with LocalSystem privileges when the service starts automatically.	7.8	More Details
CVE-2026-28615	In Telecomm, there is a possible way to initiate an unauthorized phone call due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2019-25747	Network Inventory Advisor 5.0.26.0 installs the niaservice service with an unquoted binary path that allows local attackers to escalate privileges by placing malicious executables in intermediate directories. Attackers can exploit the unquoted path in the service configuration to execute arbitrary code with LocalSystem privileges when the service starts or restarts.	7.8	More Details
CVE-2026-12957	Improper trust boundary enforcement in Language Servers for AWS before version 1.65.0 on all supported platforms may allow a for arbitrary code execution. If a local user opens a maliciously crafted workspace, any commands within the project configuration files may be automatically executed. This issue requires the user to trust the workspace when prompted. To remediate this issue, users should upgrade to Language Servers for AWS version 1.65.0 or higher.	7.8	More Details
CVE-2016-20092	NetDrive 2.6.12 contains an unquoted service path vulnerability in the Netdrive2_Service_Netdrive2 service that allows local users to execute arbitrary code with SYSTEM privileges. Attackers can insert malicious executables in the system root path that will be executed during service startup or system reboot, resulting in privilege escalation.	7.8	More Details
CVE-	In multiple locations there is a possible provisioning bypass due to improper input validation.		

2025-48643	This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2020-37254	Wondershare PDFelement 5.2.9 contains a privilege escalation vulnerability due to an unquoted service path in the WsAppService Windows service. Local attackers can place a malicious executable in the service path and execute code with LocalSystem privileges upon service restart or system reboot.	7.8	More Details
CVE-2025-48617	In overrideConfig of CarrierConfigLoader.java, there is a possible way to bypass UID check due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2020-37253	Winstep 18.06.0096 contains an unquoted service path vulnerability in the Winstep Xtreme Service that allows local attackers to escalate privileges. Attackers can place malicious executables in the Program Files directory to be executed with LocalSystem privileges when the service starts.	7.8	More Details
CVE-2020-37252	Realtek Audio Service 1.0.0.55 contains an unquoted service path vulnerability in RtkAudioService64.exe that allows local attackers to escalate privileges by injecting malicious code. Attackers can place executable files in the unquoted service path directory to execute arbitrary code with LocalSystem privileges during service startup or system reboot.	7.8	More Details
CVE-2020-37251	RealTimes Desktop Service 18.1.4 contains an unquoted service path vulnerability in the rpdsvc.exe binary that allows local attackers to escalate privileges. Attackers can place malicious executables in unquoted path directories to execute arbitrary code with LocalSystem privileges during service startup or system reboot.	7.8	More Details
CVE-2016-20093	Wise Care 365 4.27 and Wise Disk Cleaner 9.29 contain unquoted service path vulnerabilities in the WiseBootAssistant and SpyHunter 4 Service respectively, allowing local users to execute arbitrary code with SYSTEM privileges. Attackers can insert malicious executables in the system root path that execute during service startup or system reboot with elevated privileges.	7.8	More Details
CVE-2026-12112	A flaw was found in the foreman-mcp-server. A session management vulnerability in the MCP Server allows unauthenticated attackers to hijack active administrative sessions due to an improper cache of authenticated client connections, by trusting a non-secret session ID without re-validating authentication tokens and by logging all newly created session IDs to standard logs. This issue can result in privilege escalation and infrastructure-wide code execution.	7.8	More Details
CVE-2020-37250	TFTP Broadband 4.3.0.1465 contains an unquoted service path vulnerability in the tftpt.exe service binary that allows local attackers to execute arbitrary code with system privileges. Attackers can place a malicious executable in the Program Files directory path that will be executed during service startup or system reboot with LocalSystem privileges.	7.8	More Details
CVE-2016-20094	AnyDesk 2.5.0 contains an unquoted service path vulnerability that allows local users to execute arbitrary code with SYSTEM privileges by exploiting the service installation. Attackers can insert malicious executables in the system root path that execute with elevated privileges during application startup or system reboot.	7.8	More Details
CVE-2026-12786	A vulnerability has been found in Ezbsystems UltraISO Premium Edition up to 9.76. Affected by this issue is some unknown functionality in the library bootpt64.sys of the component Kernel Driver. The manipulation leads to improper access controls. Local access is required to approach this attack. 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.	7.8	More Details
CVE-2026-44274	Dell Wyse Management Suite (WMS), versions prior to WMS 2605, contain an Improper Link Resolution Before File Access vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Unauthorized access.	7.8	More Details
CVE-2026-12505	A flaw was found in the cifs-utils package where the cifs.upcall helper fails to securely drop its root privileges before looking up user information inside a user-controlled environment. A local, low privileged attacker can exploit this by using a crafted request_key payload to trick the root-owned helper into entering a custom environment (namespace) containing a malicious NSS module. This forces the system to load the attacker's controlled NSS Module and configuration, allowing them to execute arbitrary commands as the root user, elevating their privileges and fully compromising the system.	7.8	More Details

CVE-2016-20085	Realtek High Definition Audio Driver 6.0.1.6730 contains an unquoted service path vulnerability that allows local attackers to escalate privileges by placing a malicious executable in the service path. Attackers can insert an executable file in the unquoted path and restart the service to execute code with LocalSystem privileges.	7.8	More Details
CVE-2016-20087	Fortitude HTTP 1.0.4.0 contains an unquoted service path vulnerability that allows local users to execute arbitrary code with elevated privileges by exploiting the service binary path. Attackers can insert malicious executables in the system root path that execute with SYSTEM privileges during service startup or system reboot.	7.8	More Details
CVE-2026-0019	In SettingsLib, there is a possible way to disable system components due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-46461	Dell Server Hardware Manager, versions prior to 3.2.2, contains an Improper Access Control vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges.	7.8	More Details
CVE-2026-0068	In createSessionInternal of PackageInstallerService.java, there is a possible method to remove a DPC app from a managed device without DO consent due to desync from persistence. This could lead to local escalation of privilege if a user can install a malicious app with no additional execution privileges needed. User interaction is needed for exploitation.	7.8	More Details
CVE-2026-12778	A vulnerability has been found in AOMEI Partition Assistant up to 10.10.1. This vulnerability affects unknown code in the library ampa10.sys of the component Kernel Driver. Such manipulation leads to improper access controls. The attack must be carried out locally. 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.	7.8	More Details
CVE-2023-45795	A cross-site scripting vulnerability in the Builder Component of Pilz PASvisu before 1.14.1 allows a local unauthenticated attacker to inject malicious javascript and gain full control over the device.	7.8	More Details
CVE-2026-0063	In setAllowedCarriers of PhoneInterfaceManager.java, there is a possible way to disable carrier restrictions due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-0071	In SettingsLib, there is a possible missing permission check due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-12779	A vulnerability was found in AOMEI Dynamic Disk Manager up to 10.10.1. This issue affects some unknown processing in the library ddmdrv.sys of the component Kernel Driver. Performing a manipulation results in improper access controls. The attack must be initiated from a local position. 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.	7.8	More Details
CVE-2026-12780	A vulnerability was determined in AOMEI Backupper up to 8.3.0. Impacted is an unknown function in the library amwrtdrv.sys of the component Kernel Driver. Executing a manipulation can lead to improper access controls. The attack needs to be launched locally. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	7.8	More Details
CVE-2026-0081	In NFC, there is a possible way to spoof an NFC event due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2026-12781	A vulnerability was identified in EaseUS Partition Master up to 14.5. The affected element is an unknown function in the library epmntdrv.sys of the component Kernel Driver. The manipulation leads to improper access controls. The attack needs to be performed locally. The exploit is publicly available and might be used. You should upgrade the affected component. The vendor explains: "We have confirmed that this issue was present only in older versions of the product. Our product has since been updated, and the issue has been resolved in the latest version, so it no longer exists."	7.8	More Details
	Punto Switcher through 4.5.0.583 contains an unquoted search path element vulnerability that		

CVE-2026-25865	allows local attackers to execute arbitrary code by exploiting the application's call to WinExec without a fully qualified path for RunDll32.exe when invoking shell32.dll Control_RunDLL input.dll. Attackers can place a malicious executable earlier in the search order to achieve arbitrary code execution in the context of the affected user.	7.8	More Details
CVE-2026-12782	A security flaw has been discovered in EaseUS Partition Master up to 14.5. The impacted element is an unknown function in the library EUEDKEPM.sys of the component Kernel Driver. The manipulation results in improper access controls. The attack requires a local approach. The exploit has been released to the public and may be used for attacks. The affected component should be upgraded. The vendor explains: "We have confirmed that this issue was present only in older versions of the product. Our product has since been updated, and the issue has been resolved in the latest version, so it no longer exists."	7.8	More Details
CVE-2016-20088	Comodo Chromodo Browser 52.15.25.664 contains an unquoted service path vulnerability in the ChromodoUpdater service that runs with SYSTEM privileges. A local attacker can insert a malicious executable in the service path and execute arbitrary code with elevated privileges upon service restart or system reboot.	7.8	More Details
CVE-2026-12449	Use after free in Chromoting in Google Chrome on Windows prior to 149.0.7827.155 allowed a local attacker to perform OS-level privilege escalation via a malicious file. (Chromium security severity: High)	7.8	More Details
CVE-2026-54555	rtk filters and compresses command outputs before they reach your LLM context. Prior to 0.42.2, the permission splitter did not conservatively split or reject several shell constructs that Bash treats as command execution boundaries or nested execution. As a result, a command beginning with an allowed prefix such as git could hide a second command behind one of these constructs. rtk rewrite returned exit code 0, causing the Claude hook to emit permissionDecision: "allow". The rewritten command still contained the hidden command, so it ran without the user confirmation or denial that the permission rules were intended to enforce. This vulnerability is fixed in 0.42.2.	7.8	More Details
CVE-2016-20089	Iperius Remote 1.7.0 contains an unquoted service path vulnerability that allows local users to execute arbitrary code with SYSTEM privileges by exploiting the service installation path. When installed from directories containing spaces, attackers can place malicious executables in the path to be executed with elevated privileges during service startup or system reboot.	7.8	More Details
CVE-2026-0082	In tryStartActivity of NfcDispatcher.java, there is a possible automatic special app access permission assignment due to an insecure default value. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2016-20086	Vembu StoreGrid 4.0 contains an unquoted service path vulnerability in the RemoteBackup and RemoteBackup_webServer services that allows local attackers to escalate privileges. Attackers can place a malicious executable in the unquoted path and restart the service to execute code with LocalSystem privileges.	7.8	More Details
CVE-2026-54018	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.6, the SafePlaywrightURLLoader implements a validate_url function to prevent SSRF attacks by checking the IP address of the user-provided URL. However, this validation is performed only on the initial URL. Since Playwright automatically follows HTTP redirects (301/302) by default, an attacker can bypass the validation by providing a safe URL that redirects to a restricted internal network address (e.g., localhost, Docker container network, or Cloud Metadata). This allows the application to access internal services despite ENABLE_RAG_LOCAL_WEB_FETCH being set to False This vulnerability is fixed in 0.9.6.	7.7	More Details
CVE-2026-41156	Software installed and run as a non-privileged user may conduct improper GPU system calls to cause mismanagement of resources creating a write use after free scenario. A shared resource (memory page) managed by a CPU thread of control (driver) and accessed by a GPU thread of control (Firmware) can cause a write UAF when the CPU thread frees the resource before the GPU FW has finished accessing it.	7.7	More Details
CVE-2026-	Flowise before 3.1.2 contains an information disclosure vulnerability in the /api/v1/chatflows/apikey/:apikey endpoint. When the keyonly query parameter is omitted (the default), the endpoint returns not only the chatflows bound to the supplied API key but also all chatflows across every workspace that have no API key assigned, because the underlying query	7.7	More

56268	lacks any workspace filter. An attacker with a valid API key for one workspace can therefore retrieve the full ChatFlow configuration (including flowData with system prompts and node configurations, chatbotConfig, apiConfig, and credential IDs) of unprotected chatflows belonging to other workspaces.		Details
CVE-2026-54193	Contributor Arbitrary File Deletion in Fusion Builder <= 3.15.4 versions.	7.7	More Details
CVE-2026-54017	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.6, the terminal-server reverse proxy in `backend/open_webui/routers/terminals.py` does not fully confine the user-controlled `path` segment before forwarding it to an admin-configured terminal server. An authenticated user who has been granted access to a terminal server can craft `path` values containing encoded `../` traversal sequences that escape the intended path (or policy) scope on that server, reaching unintended endpoints and files on the terminal-server host. Where the terminal server fans requests out to internal services, this also gives SSRF-style reach into those services. This is a separate code path from the `/api/v1/retrieval/process/web` SSRF (GHSA-c6xv-rcvw-v685), with its own input. Two distinct vectors are consolidated here: first, raw path forwarding / single-encoded traversal (original report); and second, a bypass of the subsequently-added `_sanitize_proxy_path` mitigation using double-encoded dots (`%252e%252e`). The attacker-controlled input is the request `path`, supplied by the non-admin user, not anything an administrator configures, so this is not an admin-trust / Rule-9 situation. Version 0.9.6 fixes the issue.	7.7	More Details
CVE-2025-60223	Subscriber Arbitrary File Deletion in WPBot Pro Wordpress Chatbot <= 13.6.5 versions.	7.7	More Details
CVE-2026-32174	Improper authentication in Azure Bot Service allows an authorized attacker to elevate privileges over a network.	7.7	More Details
CVE-2026-54322	Daytona is a secure and elastic infrastructure runtime for AI-generated code execution and agent workflows. Prior to 0.185.0, Daytona's organization role update and delete endpoints authorized the caller as an owner of the organization named in the request path, but resolved and mutated the target role by its identifier alone, without verifying the role belonged to that organization. An authenticated user who owns any organization (organizations are self-service) could therefore modify the permissions of, or delete, a role belonging to a different organization, given that role's identifier. This vulnerability is fixed in 0.185.0.	7.7	More Details
CVE-2026-42129	The Loki datasource plugin's callResource handler contains a path traversal vulnerability. An authenticated Viewer-role user can escape the plugin's resource sandbox and access administrative Loki endpoints (e.g. /config, /services, /ready) to extract sensitive backend configuration and internal service information.	7.7	More Details
CVE-2026-34192	Software installed and run as a non-privileged user may conduct improper GPU system calls to cause an error path leading to UAF of GPU page tables. The vulnerability allows physical memory allocated for MMU page tables to be used after being freed. This was caused by an error path that would not cleanup properly before freeing the physical allocation.	7.7	More Details
CVE-2026-54317	Home Assistant is open source home automation software that puts local control and privacy first. Prior to 2026.6.0, the Konnected integration registers an HTTP endpoint, KonnectedView (homeassistant/components/konnected/__init__.py), that is marked as not requiring authentication (requires_auth = False). A comment next to that line says auth is instead handled "via the access token from configuration." That promise is only half true. Write requests (POST and PUT) are handled by update_sensor(), which does check the request's Authorization: Bearer <token> header against the integration's stored access tokens (using hmac.compare_digest). Read requests (GET) are handled by a separate get() method that has no authentication check at all. This vulnerability is fixed in 2026.6.0.	7.6	More Details
CVE-2026-54013	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.6, Open WebUI patched SVG XSS in user profile images and webhook profile images but forgot to apply the same fix to model profile images. The ModelMeta class has no validate_profile_image_url field validator, and the model image serving endpoint has no MIME allowlist or nosniff header. Any authenticated user with workspace.models permission (enabled	7.6	More Details

	by default) can store a ... payload in a model's profile image and achieve full account takeover of anyone who navigates to the image URL. This vulnerability is fixed in 0.9.6.		
CVE-2026-56239	Capgo before 12.128.2 contains a potential privilege escalation vulnerability in the public.apply_usage_overage SECURITY DEFINER function, which performs sensitive billing operations without enforcing internal authorization checks (no validation of auth.uid(), org membership, or check_min_rights). Because the function runs with the owner's privileges, it bypasses Row Level Security. If EXECUTE permission is available to the authenticated or anon roles (explicitly or via default privileges), an authenticated user could invoke it via Supabase RPC to manipulate billing data for arbitrary organizations, including unauthorized credit depletion and fraudulent overage event insertion.	7.6	More Details
CVE-2026-55746	Cotonti 1.0.0 (master branch, commit f43f1fc3) is vulnerable to stored Cross-Site Scripting in the Personal File Storage (PFS) module. A folder title (pff_title) is imported with the 'TXT' filter, which does not strip or encode HTML (the tag check in cot_import is disabled), so an authenticated user can store HTML/JavaScript in a folder title. In modules/pfs/inc/pfs.main.php the title is assigned to the template variable PFF_ROW_TITLE without htmlspecialchars(), and modules/pfs/tpl/pfs.tpl outputs {PFF_ROW_TITLE} unescaped. When the folder listing is viewed (including by other users for public folders), the injected script executes in the victim's browser.	7.6	More Details
CVE-2026-35327	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise Oracle WebCenter Content. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebCenter Content accessible data as well as unauthorized update, insert or delete access to some of Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N).	7.6	More Details
CVE-2026-46699	conda-smithy is a tool for combining a conda recipe with configurations to build using freely hosted CI services into a single repository. Prior to version 3.61.0, a vulnerability in the conda-forge automated webservices allowed unintended write access to feedstock repositories through GitHub username takeover. The root cause is the use of mutable GitHub usernames as identifiers for repository invitation routing, rather than stable, immutable GitHub user IDs. Version 3.61.0 fixes the issue.	7.6	More Details
CVE-2026-39546	Subscriber Privilege Escalation in MultiLoca <= 4.2.15 versions.	7.6	More Details
CVE-2026-54804	Subscriber Broken Authentication in Melhor Envio <= 2.16.3 versions.	7.6	More Details
CVE-2026-56208	A heap buffer overflow vulnerability was found in libaom, the reference AV1 codec implementation. A flaw in the AV1 encoder's Look-Ahead Processing (LAP) mode causes the first-pass stats ring buffer wrap-around guard to be bypassed when g_lag_in_frames is set to 1 or higher. This results in a 232-byte out-of-bounds write on every encoded frame after the second, corrupting adjacent heap objects. An attacker who can influence encoder configuration in a transcoding service or WebRTC session could exploit this to cause a denial of service (process crash) or potentially achieve code execution.	7.6	More Details
CVE-2026-55409	Filament is a collection of full-stack components for accelerated Laravel development. From 3.0.0 until 3.3.53, a disabled RichEditor field rendered its raw state without sanitizing HTML. Where the data stored in this field's state isn't sanitized already when the form state was filled, an attacker could plant malicious HTML or JavaScript and achieve XSS that executes for users who view the form. This vulnerability is fixed in 3.3.53.	7.6	More Details
CVE-2026-	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: VMSVGA device). The supported version that is affected is 7.2.8. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks	7.5	More

46873	may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).		Details
CVE-2025-53114	CometD is a scalable comet implementation for web messaging. In versions 5.0.0 through 5.0.22, 6.0.0 through 6.0.18, 7.0.0 through 7.0.18, and 8.0.0 through 8.0.8, bad clients that always send a fixed batch value when the server is using the acknowledgement extension may cause the unacknowledged message queue to grow indefinitely, eventually causing an `OutOfMemoryError`. Versions 5.0.23, 6.0.19, 7.0.19, and 8.0.9 patch the issue. As a workaround, disable the acknowledgement extension.	7.5	More Details
CVE-2026-35269	Vulnerability in the Identity Manager product of Oracle Fusion Middleware (component: REST WebServices). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Identity Manager. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Identity Manager accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N).	7.5	More Details
CVE-2026-11576	The security fix for CVE-2025-0728 in eclipse-threadx NetX Duo refactors error handling in the HTTP server PUT process to use a shared cleanup label, but this unified cleanup path unconditionally calls fx_file_close() even when the file was never successfully opened. Multiple error branches jump to the shared cleanup label before any file open operation has occurred, causing fx_file_close() to operate on an uninitialized file handle, leading to undefined behavior, double-close issues, or memory corruption.	7.5	More Details
CVE-2026-6734	Impact: When using Socks5ProxyAgent, undici reuses a single connection pool across different origins without verifying that the pool's origin matches the requested origin. All requests are dispatched through the pool connected to the first origin, regardless of the intended destination. This causes cross-origin request routing: credentials and request data intended for origin B are sent to origin A, responses from the wrong origin are trusted, and HTTPS requests may be silently downgraded to HTTP. Impacted users are applications that use Socks5ProxyAgent (directly or via setGlobalDispatcher) and make requests to more than one origin. This was introduced in undici 7.23.0 via PR #4385 and affects all versions through 8.1.0. Patches: Upgrade to undici v7.26.0 or v8.2.0. Workarounds: Use a separate Socks5ProxyAgent instance per origin, or avoid using Socks5ProxyAgent with multiple origins.	7.5	More Details
CVE-2026-48979	PHP Standard Library (PSL) is set of APIs covering async, collections, networking, I/O, cryptography, terminal UI, etc. In versions 6.1.0, 6.1.1 and 6.2.0, the Psl\H2\ServerConnection does not validate that the total bytes received in DATA frames match the content-length header declared in the HEADERS frame, allowing request smuggling. This is in violation of RFC 9113 §8.1.1. A malicious client is able to send more DATA bytes than declared, smuggling additional content past application-level size limits and send fewer DATA bytes than declared and close the stream early, causing applications that trust the declared length to behave incorrectly. The vulnerability is only reachable for consumers using Psl\H2\ServerConnection directly to accept untrusted client traffic. Consumers of documented high-level PSL APIs are not affected. This issue has been fixed in versions 6.1.2 and 6.2.1.	7.5	More Details
CVE-2026-48139	There is a NULL pointer dereference vulnerability in NI grpc-device in the data moniker service that may allow an attacker to cause a denial of service by triggering a crash. Successful exploitation requires an attacker to provide an unknown value to the data moniker service. This affects NI grpc-device 2.17.0 and prior versions.	7.5	More Details
CVE-2026-48818	Starlette is a lightweight ASGI framework/toolkit. In versions 1.0.1 and earlier, StaticFiles on Windows is vulnerable to SSRF. An UNC path such as \\attacker.com\share can cause os.path.realpath to initiate an outbound SMB connection before the path is rejected, exposing the service account’s NTLMv2 credentials for offline cracking or relay even though the HTTP response is only a 404. The issue affects default follow_symlink=False deployments, including frameworks built on Starlette such as FastAPI; POSIX systems and follow_symlink=True are unaffected. The issue is fixed in 1.1.0.	7.5	More Details
CVE-2026-38718	InHand Networks IR912 V1.0.0.r20042 and IR915 V1.0.0.r20042 (including earlier versions) were discovered to contain a buffer overflow vulnerability in the device registration function. This vulnerability could allow an attacker to cause a denial of service attack on the remote target	7.5	More Details

	device.		
CVE-2026-35295	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Sites. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	7.5	More Details
CVE-2026-47774	Envoy is an open source edge and service proxy designed for cloud-native applications. Prior to versions 1.35.11, 1.36.7, 1.37.3, and 1.38.1, a vulnerability in Envoy's HTTP/2 downstream request processing allows an unauthenticated remote client to trigger excessive memory consumption, potentially resulting in OOM termination of the Envoy process and denial of service. The issue arises from the combination of two behaviors. First, cookie header bytes are not fully accounted for during request header size validation in Envoy. Second, HPACK header block limits in oghttp2/quiche are enforced on encoded bytes without a corresponding limit on total decoded header size. Together, these behaviors allow a malicious client to cause large decoded header allocations while bypassing the intended request header size protections. Versions 1.35.11, 1.36.7, 1.37.3, and 1.38.1 contain a fix. No complete workaround is known short of applying a fix. Possible temporary mitigations include disabling downstream HTTP/2 where operationally feasible; enforcing stricter request header and cookie limits before traffic reaches Envoy; and monitoring Envoy memory usage for abnormal growth under HTTP/2 traffic.	7.5	More Details
CVE-2026-55203	HAProxy through 3.4.0, fixed in commit 5985276, contains an integer overflow vulnerability in the fcgi_conn structure's drl field that allows buffer misparse as new FCGI record headers. When contentLength is 65535 and paddingLength is 1 or more, the drl field wraps to 0, causing incorrect record consumption and allowing malicious FastCGI backends to desynchronize the FCGI framing parser, potentially causing request routing errors, response smuggling, or memory safety issues.	7.5	More Details
CVE-2026-55204	HAProxy through 3.4.0, fixed in commit 9a6d1fe, contains a null pointer dereference vulnerability in hpack_dht_insert() within src/hpack-tbl.c that fails to validate the return value of hpack_dht_defrag() when the memory pool is exhausted. An attacker can trigger HPACK dynamic table insertions under memory pressure to dereference a NULL pointer and crash HAProxy worker processes, causing denial of service.	7.5	More Details
CVE-2026-47633	Exposure of sensitive information to an unauthorized actor in Cost Management Interactive Experiences allows an unauthorized attacker to disclose information over a network.	7.5	More Details
CVE-2026-53754	Crawl4AI is an open-source LLM friendly web crawler & scraper. Prior to 0.8.8, the Docker API server's SSRF protection (validate_webhook_url / validate_url_destination in deploy/docker/utils.py) used an explicit IPv4/IPv6 CIDR blocklist that missed several address families. An attacker could reach internal services and cloud metadata endpoints (e.g. 169.254.169.254) despite the filter by encoding an internal IPv4 address inside an IPv6 transition form, or by using the IPv6 unspecified address. Because the Docker API is unauthenticated by default (jwt_enabled: false), no credentials are required. This vulnerability is fixed in 0.8.8.	7.5	More Details
CVE-2026-53869	Hermes Agent before 0.16.0 contains a DNS rebinding vulnerability in WebSocket endpoints that allows remote attackers to bypass Host and Origin validation. FastAPI HTTP middleware does not execute for WebSocket upgrade requests on /api/pty, /api/ws, /api/pub, and /api/events endpoints, enabling attackers to exploit DNS rebinding and inject malicious commands or read terminal output.	7.5	More Details
CVE-2026-48138	There is an out-of-bounds read vulnerability in the NI grpc-device streaming API due to a missing bounds check that may result in a denial of service. Successful exploitation requires an attacker to supply a specially crafted write request. This affects NI grpc-device 2.17.0 and prior versions.	7.5	More Details
CVE-2026-46791	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector:	7.5	More Details

	(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).		
CVE-2026-46863	Vulnerability in the MySQL Server, MySQL Cluster product of Oracle MySQL (component: Server: Connection Handling). Supported versions that are affected are MySQL Server: 8.4.0-8.4.9, 9.0.0-9.7.0; MySQL Cluster: 8.0.11-8.0.46, 8.4.0-8.4.9 and 9.0.0-9.7.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server, MySQL Cluster. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server, MySQL Cluster. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	7.5	More Details
CVE-2026-10696	Use of an incorrectly resolved name or reference in the pinget backend in Devolutions UniGetUI 2026.2.0 and earlier allows a WinGet community catalog contributor to cause an installed application to be correlated to an unrelated, attacker-controlled catalog package and to execute an attacker-controlled installer via a crafted catalog package whose normalized name is contained as a substring within the installed application name when a user applies the proposed update.	7.5	More Details
CVE-2026-46862	Vulnerability in the MySQL Router product of Oracle MySQL (component: Router: General). Supported versions that are affected are 8.4.0-8.4.9 and 9.0.0-9.7.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via TLS to compromise MySQL Router. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Router. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	7.5	More Details
CVE-2026-45617	LiquidJS is a Shopify/GitHub Pages compatible template engine written in pure JavaScript. In versions 10.25.7 and below, the built-in strip_html filter uses a regex containing four flawed lazy-quantified alternatives, leading to ReDoS via quadratic backtracking. When the input contains many <script, <style, or <!-- opener tokens without matching closers, the V8 regex engine performs O(N²) backtracking, blocking the Node.js event loop. A single ~350 KB request ('<script'.repeat(50000)) stalls the process for ~10 seconds; cost grows quadratically with input size. The default memoryLimit: Infinity does not bound regex CPU, and even when configured strip_html only charges str.length to the limit — the regex itself runs unbounded. A single unauthenticated request containing crafted untrusted input can cause severe event-loop blocking and CPU amplification that saturates Node.js workers while bypassing memoryLimit protections. This issue has been fixed in version 10.26.0.	7.5	More Details
CVE-2026-50196	Steeltoe is an open source project that provides a collection of libraries that helps users build cloud-native applications. In Steeltoe.Discovery.Eureka prior to versions 4.2.0 and 3.4.0, `DataCenterInfo.FromJson` throws `ArgumentException` for any `name` value other than `"MyOwn"` or `"Amazon"`, despite the Java Eureka specification defining a third valid value: `"Netflix"`. The exception propagates through the entire registry deserialization chain and is swallowed by the periodic cache refresh task, leaving the local service registry permanently empty or stale. Versions 4.2.0 and 3.4.0 patch the issue. If an immediate upgrade is not possible, remove any registrations using unsupported `DataCenterInfo.name` values from the registry. In mixed Java/Spring and Steeltoe environments, audit for the `Netflix` data center type before deploying Steeltoe Eureka clients.	7.5	More Details
CVE-2026-50200	Steeltoe is an open source project that provides a collection of libraries that helps users build cloud-native applications. In Steeltoe.Management.Endpoint prior to version 4.2.0 and Steeltoe.Management.EndpointCore prior to version 3.4.0, the `Sanitizer` component in the Environment actuator redacts configuration values by matching the configuration key name against a suffix list. The default list (`password`, `secret`, `key`, `token`, `.*credentials.*`, `vcap_services`) does not cover the standard .NET pattern `ConnectionStrings:<name>` or Steeltoe Connectors' `Steeltoe:Client:<type>:Default:ConnectionString`. There is no value-based scrubbing, so full connection string values including embedded `Password=` and `user:pass@host` segments are returned verbatim in `/actuator/env` responses. Steeltoe.Management.Endpoint 4.2.0 and Steeltoe.Management.EndpointCore 3.4.0 patch the issue. If an immediate upgrade is not possible: On the standard path, remove `env` from the actuator exposure list; add `.*connectionstring.*` to `KeysToSanitize` as a defense-in-depth measure for both paths; and/or require authorization on actuator endpoints.	7.5	More Details
CVE-2026-8050	In SignalRGB versions prior to 1.3.7.0, seven of the thirteen IOCTL handlers dereference the SystemBuffer pointer without first verifying that it is non-NULL. Sending an IOCTL with an empty input buffer causes a NULL pointer dereference, resulting in a kernel crash.	7.5	More Details

CVE-2026-35275	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Shared Folders). The supported version that is affected is 7.2.8. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle VM VirtualBox accessible data as well as unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:N).	7.5	More Details
CVE-2026-45357	LiquidJS is a Shopify/GitHub Pages compatible template engine written in pure JavaScript. In versions 10.25.7 and below, the date filter's strftime implementation parses width specifiers like %9999999d and forwards the captured width unchecked into pad()/padStart(), leading to memory and render limit bypass. In src/util/underscore.ts, the pad loop performs unbounded string concatenation without consulting the Context's memoryLimit or renderLimit, so a single small template ({{ x | date: '%5000000d' }}) produces megabytes of output and unbounded CPU. The memoryLimit and renderLimit options the docs (src/liquid-options.ts:87-92) advertise as DoS controls — and which the docstring explicitly mentions for strftime — are entirely bypassed. Exploitation can cause large memory allocations, high CPU usage, or OOM crashes per render. This issue has been fixed in version 10.26.0.	7.5	More Details
CVE-2026-52844	Caddy is an extensible server platform that uses TLS by default. Prior to 2.11.4, on Windows, Caddy path matchers treat /private\secret.txt as outside /private/*, but file_server later resolves the same request path as private\secret.txt on disk. An unauthenticated remote client can bypass Caddy path-scoped auth/deny routes protecting /private/*. This vulnerability is fixed in 2.11.4.	7.5	More Details
CVE-2026-54417	An integer overflow in the mtar_next() function in src/microtar.c in rxi microtar 0.1.0 allows a remote attacker to cause a denial of service (uncontrolled CPU consumption / infinite loop) via a crafted tar archive. mtar_next() computes the offset to the next record as round_up(h.size, 512) + sizeof(mtar_raw_header_t) using 32-bit arithmetic. When the header size field is a multiple of 512 in the range 0xFFFFFC01-0xFFFFFE00 (e.g. 0xFFFFFE00), the addition wraps to 0, so mtar_next() seeks to the current record position instead of advancing. As a result, mtar_find() and any loop that iterates entries with mtar_next() repeat indefinitely over the same record, hanging the process at 100% CPU with no recovery.	7.5	More Details
CVE-2026-8858	IBM i 7.6, 7.5, 7.4, and 7.3, IBM WebSphere Application Server and IBM WebSphere Application Server Liberty are vulnerable to remote code execution and denial of service in the WebSphere Web Server Plug-in component. This vulnerability can be exploited when an attacker impersonates the application server and sends crafted responses to the plug-in.	7.5	More Details
CVE-2025-61029	An issue in the sqlo_untry component of openlink virtuoso-opensource v7.2.11 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.	7.5	More Details
CVE-2026-56253	Capgo before 12.128.2 contains an improper access control vulnerability in the public.get_org_members RPC function that allows unauthenticated attackers to enumerate organization members. Attackers can invoke the endpoint using only the public sb_publishable_* key and an organization UUID to retrieve sensitive member information including email addresses, user IDs, roles, and pending invitations.	7.5	More Details
CVE-2026-48511	MessagePack for C# is a MessagePack serializer for C#. Prior to 2.5.301 and 3.1.7, ExpandoObjectFormatter.Deserialize populates System.Dynamic.ExpandoObject by calling IDictionary<string, object>.Add for each map entry. ExpandoObject internally maintains member names in array-like structures, so inserting many distinct keys can require repeated linear scans and array copies. For large attacker-controlled maps, this produces quadratic CPU and allocation behavior. The issue is especially surprising because ExpandoObjectResolver.Options is configured with MessagePackSecurity.UntrustedData, but collision-resistant dictionary comparers cannot protect ExpandoObject insertion internals. This vulnerability is fixed in 2.5.301 and 3.1.7.	7.5	More Details
	MessagePack for C# is a MessagePack serializer for C#. Prior to 2.5.301 and 3.1.7, MessagePack-CSharp's JSON conversion helpers contain multiple recursion paths that do not consistently enforce a depth limit. These paths are in the JSON conversion component rather		

CVE-2026-48512	than normal typed MessagePack deserialization. MessagePackSerializer.ConvertFromJson recursively processes nested JSON arrays and objects in FromJsonCore() without consulting MessagePackSecurity.MaximumObjectGraphDepth. TinyJsonReader.ReadNextToken() recursively consumes comma and colon separator characters, allowing even malformed JSON with long separator runs to consume one stack frame per character. MessagePackSerializer.ConvertToJson applies depth checks to arrays and maps, but the typeless extension branch for ext-100 recursively calls ToJsonCore() without applying MessagePackSecurity.DepthStep(ref reader). Each path can allow attacker-controlled input to exhaust the process stack and trigger an uncatchable StackOverflowException instead of failing with a catchable parse or serialization exception. This vulnerability is fixed in 2.5.301 and 3.1.7.	7.5	More Details
CVE-2026-48513	MessagePack for C# is a MessagePack serializer for C#. Prior to 2.5.301 and 3.1.7, runtime-generated union deserializers emitted by DynamicUnionResolver do not call MessagePackSecurity.DepthStep(ref reader) and do not decrement reader.Depth around recursive deserialization and skip paths. This means union deserialization does not consistently participate in the maximum object graph depth enforcement that protects other recursive formatter paths. For unknown union keys, the emitted deserializer calls reader.Skip() on attacker-controlled data without an enclosing depth step. This vulnerability is fixed in 2.5.301 and 3.1.7.	7.5	More Details
CVE-2026-48514	MessagePack for C# is a MessagePack serializer for C#. Prior to 2.5.301 and 3.1.7, UnsafeBlitFormatterBase<T>.Deserialize reads an attacker-controlled byteLength from an extension payload and allocates an array based on that value before validating it against the extension header length or remaining payload bytes. The outer extension header is bounded by available input, but that bound is not used to constrain the inner byteLength before allocation. A very small payload can therefore request a very large T[] allocation. This vulnerability is fixed in 2.5.301 and 3.1.7.	7.5	More Details
CVE-2026-48515	MessagePack for C# is a MessagePack serializer for C#. Prior to 2.5.301 and 3.1.7, MessagePack-CSharp's multi-dimensional array formatters read dimension lengths directly from the payload and allocate T[,], T[,,], or T[,,,] before validating that the dimension product matches the encoded element count. The formatter reads a guarded element array header, but allocation of the target multi-dimensional array happens before the dimensions are checked against that element count. A small payload can therefore declare large dimensions, provide an empty or tiny inner array, and cause a large heap allocation before element data is validated. This vulnerability is fixed in 2.5.301 and 3.1.7.	7.5	More Details
CVE-2026-48516	MessagePack for C# is a MessagePack serializer for C#. Prior to 2.5.301 and 3.1.7, InterfaceLookupFormatter<TKey,TElement> constructs an internal Dictionary<TKey, IGrouping<TKey,TElement>> with the default equality comparer instead of the security-aware comparer supplied by options.Security.GetEqualityComparer<TKey>(). This formatter omission allows hash-collision CPU denial of service against ILookup<TKey,TElement> even when the application has opted into the untrusted-data security posture This vulnerability is fixed in 2.5.301 and 3.1.7.	7.5	More Details
CVE-2026-48517	MessagePack for C# is a MessagePack serializer for C#. Prior to 2.5.301 and 3.1.7, MessagePack-CSharp's typeless deserialization includes MessagePackSerializerOptions.ThrowIfDeserializingTypeIsDisallowed(Type) as a safety check for dangerous types. The default implementation checks the outer type name, but it does not recursively inspect array element types or generic type arguments. As a result, a type that would be blocked directly can be wrapped inside an array or constructed generic type and pass the outer type check. The formatter machinery can then materialize formatters for the inner blocked type. This vulnerability is fixed in 2.5.301 and 3.1.7.	7.5	More Details
CVE-2026-56323	Capgo before 12.128.2 contains an information disclosure vulnerability in the /functions/v1/channel_self endpoint that allows unauthenticated attackers to enumerate non-public channel names and determine app existence and subscription status. Remote attackers can send GET requests with arbitrary app_id parameters to disclose internal rollout channels, enumerate valid applications across tenants, and leak billing status without authentication or device binding.	7.5	More Details
CVE-2026-	Capgo before 12.128.2 contains an unauthenticated security definer RPC function get_identity_apikey_only that returns the owning user_id for supplied API keys, creating an API key validity oracle and user identity disclosure primitive. Attackers can call this endpoint with	7.5	More

56242	valid or invalid API keys to confirm key validity and map keys to user identifiers, then chain results into other exposed RPCs like get_orgs_v6 to retrieve organization membership and management email PII.		Details
CVE-2026-56082	Capgo (Cap-go/capgo) before 12.128.2 contains an improper access control vulnerability in the SECURITY DEFINER PostgREST RPC function public.record_build_time, which is granted to the anon role and callable with only the public Supabase publishable (sb_publishable_*) anon key. An unauthenticated attacker can insert rows into public.build_logs for arbitrary organizations and, because the function uses ON CONFLICT (build_id, org_id) DO UPDATE, can overwrite existing usage/billing records by reusing the same build_id for a target org. This enables cross-tenant tampering of billing build logs and financial-impact denial of service by inflating billable build time.	7.5	More Details
CVE-2026-48779	ws is an open source WebSocket client and server for Node.js. All versions from 1.1.0 up to (but not including) 5.2.5, from 6.0.0 up to 6.2.4, from 7.0.0 up to 7.5.11, and from 8.0.0 up to 8.21.0 are affected by a memory exhaustion DoS vulnerability. A peer can send a high volume of exceptionally small fragments and data chunks, with modest network traffic, to force the remote peer into allocating and holding structural wrappers that consume far more memory than the default documented message-size limit, leading to process termination due to OOM. This issue has been fixed in versions 5.2.5, 6.2.4, 7.5.11, and 8.21.0.	7.5	More Details
CVE-2026-49057	Unauthenticated Broken Access Control in JobSearch <= 3.2.7 versions.	7.5	More Details
CVE-2026-41523	vLLM is an inference and serving engine for large language models (LLMs). Prior to 0.22.0, an assert-based security check in vLLM's activation function loading allows any unauthenticated attacker to achieve arbitrary code execution on the server by publishing a malicious HuggingFace model, when vLLM runs in Python optimized mode (python -O or PYTHONOPTIMIZE=1). This vulnerability is fixed in 0.22.0.	7.5	More Details
CVE-2026-56341	AVideo through version 26.0 contains multiple unauthenticated list.json.php endpoints in payment plugins lacking authorization checks, exposing PayPal tokens, Authorize.Net webhooks, and Bitcoin transaction records. Unauthenticated attackers can retrieve all payment transaction data including agreement IDs, user financial records, and API responses via direct GET requests to vulnerable endpoints.	7.5	More Details
CVE-2026-52696	Unauthenticated Sensitive Data Exposure in JetBlog <= 2.4.8 versions.	7.5	More Details
CVE-2020-37255	WordPress Time Capsule Plugin 1.21.16 contains an authentication bypass vulnerability that allows unauthenticated attackers to gain administrative access by sending a crafted POST request with the IWP_JSON_PREFIX header. Attackers can exploit this flaw to obtain valid administrator session cookies and access the WordPress dashboard without providing credentials.	7.5	More Details
CVE-2026-11912	The Simple File List plugin for WordPress is vulnerable to arbitrary file modification due to insufficient authorization checks in all versions up to, and including, 6.3.7. This makes it possible for unauthenticated attackers to delete and modify files on the serve. This vulnerability is exploitable even when the administrator has not enabled the AllowFrontManage setting, because the is_admin() check unconditionally short-circuits the guard before that setting is evaluated.	7.5	More Details
CVE-2026-11911	The Simple File List plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the eeSFL_DeleteFile function in all versions up to, and including, 6.3.7. This makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php). The simplefilelist_edit_job AJAX action is registered via wp_ajax_nopriv_, making it accessible without authentication, and the is_admin() guard that would otherwise restrict access is bypassed because is_admin() always returns true for requests to the admin-ajax.php endpoint.	7.5	More Details
CVE-2026-	MessagePack for C# is a MessagePack serializer for C#. Prior to 2.5.301 and 3.1.7, when MessagePack-CSharp decompresses Lz4Block or Lz4BlockArray payloads, it reads declared uncompressed lengths from the wire and allocates output buffers based on those lengths before validating that the compressed data is valid or that the declared expansion is reasonable. A	7.5	More Details

48510	small payload can claim a very large uncompressed length and force a large allocation before LZ4 decoding begins. This vulnerability is fixed in 2.5.301 and 3.1.7.		
CVE-2026-12360	The JetEngine plugin for WordPress is vulnerable to SQL injection in all versions up to and including 3.8.10.1. The listing_load_more AJAX handler accepts a filtered_query parameter that is intentionally excluded from the HMAC query signature check to support front-end filter integration. However, meta_query row values within filtered_query are not sanitized before being merged into SQL construction. This makes it possible for unauthenticated attackers to perform time-based or boolean blind SQL injection by appending a malicious meta_query value to a Load More AJAX request captured from any public Listing Grid page.	7.5	More Details
CVE-2026-48506	MessagePack for C# is a MessagePack serializer for C#. Prior to 2.5.301 and 3.1.7, MessagePackReader.TrySkip() recursively descends into nested arrays and maps without incrementing the reader depth or calling the configured depth checks. This bypasses MessagePackSecurity.MaximumObjectGraphDepth, the library's documented protection against deeply nested object graphs. Many generated and dynamic formatters call reader.Skip() when they encounter unknown map keys, unknown array members, ignored fields, or data that should be skipped for forward compatibility. A deeply nested value in one of these skipped positions can therefore cause unbounded recursion and an uncatchable StackOverflowException. This vulnerability is fixed in 2.5.301 and 3.1.7.	7.5	More Details
CVE-2026-12445	Use after free in Extensions in Google Chrome prior to 149.0.7827.155 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension. (Chromium security severity: High)	7.5	More Details
CVE-2026-34888	Unauthenticated Sensitive Data Exposure in Bricksforge <= 3.1.8.4 versions.	7.5	More Details
CVE-2026-9071	IBM WebSphere Application Server 9.0, and 8.5 and IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.6 are vulnerable to a denial of service, caused by sending a specially-crafted request. A remote attacker could exploit this vulnerability to cause the server to consume memory resources.	7.5	More Details
CVE-2026-42127	The public dashboard query endpoint does not limit request body size before processing, allowing unauthenticated attackers to trigger excessive memory allocation by sending arbitrarily large JSON payloads. This can lead to denial of service through memory exhaustion. No valid dashboard access token or authentication is required to exploit this vulnerability.	7.5	More Details
CVE-2026-48712	protobufjs compiles protobuf definitions into JavaScript (JS) functions. Prior to 7.6.1 and 8.4.1, protobufjs could recurse without a depth limit while converting decoded messages to plain objects or JSON. This affected generated toObject() conversion and the custom google.protobuf.Any JSON conversion path. A crafted protobuf binary payload containing deeply nested Any values could cause the JavaScript call stack to be exhausted during conversion to JSON. This vulnerability is fixed in 7.6.1 and 8.4.1.	7.5	More Details
CVE-2026-53539	Python-Multipart is a streaming multipart parser for Python. Prior to 0.0.30, when parsing application/x-www-form-urlencoded bodies, QuerystringParser located the field separator with a two step lookup: it first scanned the entire remaining buffer for &, and only when no & existed anywhere ahead did it fall back to scanning for ;. For a body that uses ; as the separator and contains no &, every field iteration performed a full failed & scan over the entire remaining buffer before locating the nearby ;. With N semicolon separated fields in a chunk of size B, this yields O(B^2) byte comparisons per chunk. An attacker can submit a small crafted body of the form a;a;a;... and cause the parser to spend seconds of CPU per request. A handful of concurrent requests can exhaust worker processes. This vulnerability is fixed in 0.0.30.	7.5	More Details
CVE-2026-54283	Starlette is a lightweight ASGI framework/toolkit. From 0.4.1 until 1.3.1, request.form() accepts max_fields and max_part_size to bound resource consumption while parsing form data. These limits are enforced for multipart/form-data, but silently ignored for application/x-www-form-urlencoded. An unauthenticated attacker can therefore send a urlencoded body with an arbitrarily large number of fields or an arbitrarily large field, even when the application configured limits it believed would apply. This vulnerability is fixed in 1.3.1.	7.5	More Details
CVE-2026-	Subscriber Arbitrary File Download in Woocommerce Book Price <= 1.3 versions.	7.5	More

22334			Details
CVE-2026-53779	WebP Server Go through 0.14.4 contains a path traversal vulnerability on Windows that allows unauthenticated attackers to read files outside the configured IMG_PATH directory by sending requests with percent-encoded backslashes (%5C) that bypass the path.Clean() sanitization in handler/router.go. Attackers can exploit the discrepancy between Go's forward-slash-only path normalization and Windows file system APIs that treat backslashes and forward slashes as equivalent to access arbitrary files on the host filesystem accessible to the server process.	7.5	More Details
CVE-2026-54293	NLTK (Natural Language Toolkit) is a suite of open source Python modules, data sets, and tutorials supporting research and development in Natural Language Processing. Prior to 3.10.0-rc1, nltk.data.load() in NLTK is vulnerable to path traversal via URL-encoded path separators and traversal segments when using the nltk: URL scheme. The unsafe-path regex check is performed before url2pathname() decodes the %xx sequences (a classic decode-after-check / TOCTOU-style flaw), allowing an attacker to bypass the protection documented in NLTK's SECURITY.md and read arbitrary files from the filesystem. While literal traversal strings such as ../../../etc/passwd are correctly blocked, encoded variants such as %2fetc%2fpasswd, %2e%2e%2f..., and ..%2f..%2f slip past the regex and are subsequently decoded into a real filesystem path. This vulnerability is fixed in 3.10.0-rc1.	7.5	More Details
CVE-2026-54299	Astro is a web framework. Prior to 6.4.6, Astro SSR apps with prerendered error pages (/404 or /500 using export const prerender = true) fetch those pages over HTTP at runtime when an error occurs. The URL for this fetch is derived from request.url, which in turn gets its origin from the incoming Host header. When the Host header is not validated against allowedDomains, an attacker can point the fetch at an arbitrary host and read the response. This vulnerability is fixed in 6.4.6.	7.5	More Details
CVE-2026-12462	Use after free in Media in Google Chrome prior to 149.0.7827.155 allowed a remote attacker who had compromised the renderer process to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	7.5	More Details
CVE-2026-55603	http-proxy-middleware is node.js http-proxy middleware. From 3.0.4 until 3.0.7 and 4.1.1, fixRequestBody() is the library's documented helper for re-emitting a request body that was already consumed by a body parser. When the outgoing Content-Type is multipart/form-data, it rebuilds the body with handlerFormDataBodyData(), which interpolates each req.body key and value directly into the multipart wire format without neutralizing CR/LF. A \r\n inside a value (or key) lets an attacker close the current part and inject an entirely new form part. Because the proxy's own body parser saw a single opaque value, any gateway-side policy or validation performed on req.body is evaluated against a different set of fields than the upstream backend ultimately parses a request/parameter desynchronization across the trust boundary. This vulnerability is fixed in 3.0.7 and 4.1.1.	7.5	More Details
CVE-2026-40721	Contributor Local File Inclusion in Element Pack Pro <= 9.0.6 versions.	7.5	More Details
CVE-2025-66389	GitHub Copilot 1.372.0 allows filesystem access outside of a workspace folder (without user approval) via a file-handler URI parameter to fetch_webpage. Therefore, exfiltration could occur if there is indirect prompt injection.	7.5	More Details
CVE-2026-12581	EasyFlow .NET developed by Digiwin has a Session Fixation vulnerability. If unauthenticated remote attackers replace a specific session ID for a user, they can gain the user's privilege once the user logs in.	7.5	More Details
CVE-2026-12455	Use after free in Tab Strip in Google Chrome prior to 149.0.7827.155 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	7.5	More Details
CVE-2026-48502	MessagePack for C# is a MessagePack serializer for C#. Prior to 2.5.301 and 3.1.7, MessagePackReader.ReadDateTime() can allocate stack memory based on an attacker-controlled MessagePack extension length. In the slow path for timestamp extension parsing, the computed tokenSize includes the extension body length from the wire and is used in a stackalloc operation before the extension length is validated as one of the valid timestamp sizes. A very small payload can claim a large timestamp extension body and cause a stack allocation large enough to trigger an uncatchable StackOverflowException, terminating the host process. This	7.5	More Details

	vulnerability is fixed in 2.5.301 and 3.1.7.		
CVE-2026-56214	Capgo before 12.128.2 contains an information disclosure vulnerability in Supabase PostgREST RPC endpoints is_trial_org and is_paying_org that allows unauthenticated attackers to enumerate organizations and disclose billing status using the public sb_publishable key. Attackers can invoke these endpoints to determine organization existence via distinguishable return values and identify paying customers for targeted profiling.	7.5	More Details
CVE-2026-54802	Unauthenticated Broken Authentication in SMS Alert Order Notifications <= 3.9.3 versions.	7.5	More Details
CVE-2026-50559	Quarkus is a Java framework for building cloud-native applications. Prior to versions 3.37.0, 3.36.3, 3.33.2.1, 3.33.3, 3.27.4.1, 3.27.5, and 3.20.6.2, Quarkus HTTP path-based authorization policies can be bypassed using encoded semicolons (%3B) to smuggle matrix parameters past the security layer, and using encoded slashes (%2F) or backslashes (%5C) to access protected static resources. This is a distinct issue from CVE-2026-39852, which addressed only literal semicolon stripping. Versions 3.37.0, 3.36.3, 3.33.2.1, 3.33.3, 3.27.4.1, 3.27.5, and 3.20.6.2 contain a patch.	7.5	More Details
CVE-2025-61020	An issue in the sqlo_strip_in_join component of openlink virtuoso-opensource v7.2.11 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.	7.5	More Details
CVE-2026-54810	Missing Authorization vulnerability in Nexi Payments Nexi XPay allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Nexi XPay: from n/a through 8.3.1.	7.5	More Details
CVE-2026-46974	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.2.8. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).	7.5	More Details
CVE-2026-46971	Vulnerability in the Oracle HR Intelligence product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle HR Intelligence. Successful attacks of this vulnerability can result in takeover of Oracle HR Intelligence. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	7.5	More Details
CVE-2026-12151	Impact: The undici WebSocket client enforces maxPayloadSize on the cumulative byte count of fragments in a message but does not enforce a limit on the number of fragments. A malicious WebSocket server can stream many small or empty continuation frames that each pass per-frame and cumulative-size validation, collectively causing unbounded memory growth in the client process. The result is memory exhaustion and a denial of service. Affected applications are those using the undici WebSocket client (new WebSocket(...)) or the WebSocketStream API that can be induced to connect to an attacker-controlled or compromised WebSocket endpoint. All releases starting at undici 6.17.0 are affected. Patches: Upgrade to undici >= 6.26.0, >= 7.28.0, or >= 8.5.0. Workarounds: No workaround is available. The fix must be applied through an upgrade.	7.5	More Details
CVE-2026-13007	Tenable Identity Exposure contains multiple unauthenticated API endpoints under /w/api/* that expose sensitive application configuration data including cleartext LDAP credentials, SAML configuration, user accounts, and directory settings to unauthenticated remote attackers. Affected responses are served with Cache-Control: public headers and without Vary: Cookie, allowing reverse proxies and CDNs to cache and serve sensitive data to unauthenticated users even after authentication is applied.	7.5	More Details
CVE-2026-46966	Vulnerability in the Oracle Universal Work Queue product of Oracle E-Business Suite (component: Work Provider Site Level Administration). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Universal Work Queue. Successful attacks of this vulnerability can result in takeover of Oracle Universal Work Queue. CVSS 3.1 Base Score 7.5	7.5	More Details

	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).		
CVE-2026-20190	A vulnerability in Cisco ISE and ISE-PIC could allow an unauthenticated, remote attacker to view sensitive information on an affected device. This vulnerability is due to improper authorization checks when a resource is accessed. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to gain access to sensitive information, including hashed credentials that could be used in future attacks.	7.5	More Details
CVE-2026-46959	Vulnerability in the Oracle Subledger Accounting product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Subledger Accounting. Successful attacks of this vulnerability can result in takeover of Oracle Subledger Accounting. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	7.5	More Details
CVE-2026-46958	Vulnerability in the Oracle Subledger Accounting product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Subledger Accounting. Successful attacks of this vulnerability can result in takeover of Oracle Subledger Accounting. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	7.5	More Details
CVE-2026-46957	Vulnerability in the Oracle iSupplier Portal product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle iSupplier Portal. Successful attacks of this vulnerability can result in takeover of Oracle iSupplier Portal. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	7.5	More Details
CVE-2026-46955	Vulnerability in the Oracle Human Resources product of Oracle E-Business Suite (component: Person). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Human Resources. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle Human Resources. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H).	7.5	More Details
CVE-2026-53872	picklescan before 0.0.35 contains an unsafe pickle deserialization vulnerability allowing unauthenticated attackers to read arbitrary server files by chaining io.FileIO and urllib.request.urlopen. Attackers can bypass RCE-focused blocklists to exfiltrate sensitive data like /etc/passwd to external servers.	7.5	More Details
CVE-2026-55446	Langflow is a tool for building and deploying AI-powered agents and workflows. Prior to 1.0.19, an attacker can send a /api/v1/files/upload/ request without any authentication token/cookies and abuse a very long multipart form boundary to make the langflow app unusable for all users for an indefinite amount of time. This vulnerability is fixed in 1.0.19.	7.5	More Details
CVE-2026-9675	Impact: The undici WebSocket client enforces maxPayloadSize per-frame but does not enforce the cumulative size of fragmented uncompressed messages. A malicious WebSocket server can stream many small fragments that each pass per-frame validation but collectively exceed the configured limit, causing unbounded memory growth in the client process. The result is memory exhaustion and a denial of service. Affected applications are those using the undici WebSocket client (new WebSocket(...)) that can be induced to connect to an attacker-controlled or compromised WebSocket endpoint. This is a regression specific to undici 8.1.0. The 6.25.0 line shipped the equivalent cumulative check from the start and is unaffected. The 7.x line never had the maxPayloadSize feature and is also unaffected. Patches: Upgrade to undici >= 8.5.0. Workarounds: No workaround is available. The fix must be applied through an upgrade.	7.5	More Details
CVE-2026-46935	Vulnerability in the Oracle Complex Maintenance, Repair and Overhaul product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair and Overhaul. Successful attacks of this vulnerability can result in takeover of Oracle Complex Maintenance, Repair and Overhaul. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	7.5	More Details

CVE-2026-46934	Vulnerability in the Oracle Complex Maintenance, Repair and Overhaul product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair and Overhaul. Successful attacks of this vulnerability can result in takeover of Oracle Complex Maintenance, Repair and Overhaul. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	7.5	More Details
CVE-2025-61024	An issue in the sqlo_try_in_loop component of openlink virtuoso-opensource v7.2.11 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.	7.5	More Details
CVE-2025-61025	An issue in the sslr_qst_get component of openlink virtuoso-opensource v7.2.11 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.	7.5	More Details
CVE-2025-61022	An issue in the sqlo_tb_col_preds component of openlink virtuoso-opensource v7.2.11 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.	7.5	More Details
CVE-2025-61018	An issue in the sqlo_place_dt_set component of openlink virtuoso-opensource v7.2.11 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.	7.5	More Details
CVE-2025-49403	Unauthenticated Arbitrary File Download in Premium Age Verification / Restriction for WordPress <= 3.0.2 versions.	7.5	More Details
CVE-2026-48774	ProxySQL is a proxy for MySQL and its forks, as well as PostgreSQL. In versions 3.0.0 through 3.0.8, ProxySQL's GenAI/MCP `run_sql_readonly` tool violates its documented read-only contract for MySQL targets. The tool validates only the full input string with a substring blacklist and first-keyword allowlist, but then executes the entire SQL string on a backend connection created with `CLIENT_MULTI_STATEMENTS`. As a result, a caller can submit a read-only first statement followed by a side-effecting second statement, such as `SELECT 1; RENAME TABLE ...`. The validator accepts the payload because it starts with `SELECT` and because side-effecting MySQL statements such as `RENAME TABLE`, `SET`, `RESET`, `LOCK TABLES`, and `KILL` are not rejected by the blacklist. In a live MCP runtime test, the `/mcp/query` endpoint accepted a `run_sql_readonly` request. The MCP response reported success for the first `SELECT`, and direct backend verification showed that the table had actually been renamed. This violates the endpoint's read-only security contract and lets an MCP caller perform backend writes or administrative SQL, limited by the configured MCP target account's database privileges. Version 3.0.9 contains a fix. Other operator mitigations include: keeping MCP disabled unless required; setting a non-empty `mcp-query_endpoint_auth` token before exposing `/mcp/query`; restricting MCP listener network exposure; configuring MCP backend target credentials as database-level read-only users; and adding temporary MCP query rules to block obvious multi-statement patterns.	7.5	More Details
CVE-2026-49293	js-toml is a TOML parser for JavaScript, fully compliant with the TOML 1.0.0 Spec. Versions up to and including 1.1.0 parse hexadecimal / octal / binary integer literals via a hand-written `parseBigInt` loop that multiplies a `BigInt` accumulator by the radix once per input digit. Each iteration performs a `BigInt * BigInt` operation on an accumulator that grows linearly with the number of digits already consumed, so the whole loop is $O(n^2)$ in the literal length. The lexer regex places no upper bound on the literal length, so a single TOML document containing one ~500 kB hex literal pins one CPU core for ~40 seconds on a modern laptop (Apple M-series, Node v22). Memory amplification is bounded but CPU amplification is severe and grows quadratically: doubling the literal length quadruples the work. A caller that invokes `load()` on attacker-controlled TOML (configuration upload endpoints, CI/CD systems ingesting third-party `*.toml`, IDE plugins, build tools) is exposed to a single-request CPU exhaustion DoS. Version 1.1.1 fixes the issue.	7.5	More Details
CVE-2023-54357	Joomla com_booking component 2.4.9 contains an information disclosure vulnerability that allows unauthenticated attackers to enumerate user accounts by exploiting the getUserData function in the customer controller. Attackers can send GET requests to index.php with option=com_booking, controller=customer, task=getUserData, and an id parameter to retrieve	7.5	More Details

	user names, usernames, and email addresses through brute force enumeration.		
CVE-2026-9690	Unauthenticated Arbitrary File Download in WP Media folder Addon <= 4.0.1 versions.	7.5	More Details
CVE-2019-25762	Joomla! Component JoomProject 1.1.3.2 contains an information disclosure vulnerability that allows unauthenticated attackers to access sensitive user data by exploiting the projects endpoint. Attackers can send requests to index.php with option=com_jpprojects&view=projects&tmpl=component&format=json parameters to retrieve user IDs, names, and email addresses in JSON format.	7.5	More Details
CVE-2025-69131	Unauthenticated Arbitrary File Download in WordPress & WooCommerce Scraper Plugin, Import Data from Any Site <= 1.0.7 versions.	7.5	More Details
CVE-2026-8379	The Frontend File Manager Plugin WordPress plugin through 23.6 does not properly enforce its nonce check on the file download handler, allowing unauthenticated attackers to download files uploaded by any user through the Frontend File Manager Plugin WordPress plugin through 23.6 by iterating identifiers.	7.5	More Details
CVE-2025-69103	Subscriber Arbitrary Content Deletion in Brikk <= 3.0.0 versions.	7.5	More Details
CVE-2023-54365	Traefik before 2.10.5 and 3.0.0-beta4 is affected by a denial-of-service vulnerability in HTTP/2 request handling inherited from the Go standard library's HTTP/2 implementation (CVE-2023-44487 / CVE-2023-39325, the 'Rapid Reset' technique). A remote attacker can rapidly create and cancel HTTP/2 streams to exhaust server resources and cause service unavailability.	7.5	More Details
CVE-2026-54816	Improper Control of Generation of Code ('Code Injection') vulnerability in Monetizemore Advanced Ads allows Remote Code Inclusion. This issue affects Advanced Ads: from n/a through 2.0.21.	7.5	More Details
CVE-2026-22283	Dell PowerFlex Manager, version(s) Version prior to 4.8, contain(s) an Inclusion of Functionality from Untrusted Control Sphere vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Information disclosure.	7.5	More Details
CVE-2026-56248	Cap-go capgo (capgo-backend) before 12.128.12 contains an unauthenticated denial-of-service vulnerability arising from the audit_logs table's Row-Level Security (RLS) policy when accessed via the Supabase PostgREST API. Because the PostgreSQL query planner executes costly logic before RLS rejection, unfiltered queries to the public.audit_logs endpoint using the public anon key consistently trigger statement timeouts (PostgREST error 57014). Under concurrency, this exhausts database resources and causes cascading HTTP 500 failures on unrelated endpoints (e.g. /orgs), resulting in an application-layer denial of service.	7.5	More Details
CVE-2026-56322	Capgo before 12.128.2 contains an information disclosure vulnerability in the unauthenticated /updates endpoint that resolves the defaultChannel parameter before enforcing privacy restrictions, allowing attackers to enumerate private channels and leak version/config state. Unauthenticated attackers can probe private channel names and distinguish valid channels from nonexistent ones based on response differences, revealing assigned bundle versions and platform-specific configuration details.	7.5	More Details
CVE-2024-32729	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in QuantumCloud Conversational Forms for ChatBot allows Path Traversal. This issue affects Conversational Forms for ChatBot: from n/a through 1.1.8.	7.5	More Details
CVE-2026-44726	Deno is a JavaScript, TypeScript, and WebAssembly runtime. From 2.0.0 until 2.7.8, a flaw in Deno's Node.js tls compatibility layer could cause a TLS client to transmit application data in plaintext after a connection retry. When `autoSelectFamily was enabled and the first address-family attempt failed, the socket reinitialization path reused a stale TLS upgrade hook that was bound to the original, failed handle. As a result, the replacement TCP connection was never upgraded to TLS, and any data the application wrote before the secureConnect event travelled over the network unencrypted. A network attacker positioned to cause the initial connection attempt to fail (for example, by dropping IPv6 traffic on a dual-stack host) could deterministically trigger the fallback path and observe or tamper with traffic that the application believed was	7.4	More Details

	TLS-protected. This vulnerability is fixed in 2.7.8.		
CVE-2026-49440	Deno is a JavaScript, TypeScript, and WebAssembly runtime. Prior to 2.8.1, node:crypto.checkPrime(candidate[, options][, callback]) and crypto.checkPrimeSync(candidate[, options]) ran no Miller-Rabin rounds at all when the caller left options.checks at its default of 0. In that mode, the only test applied to the candidate was trial division by the primes up to 17,863. Any composite whose smallest prime factor exceeds that bound — for example the product of two primes just above it, such as 17,881 × 17,891 — was reported as true ("probably prime"). The same divergence affected the lower-level op_node_check_prime / op_node_check_prime_bytes paths that the polyfill calls into. This vulnerability is fixed in 2.8.1.	7.4	More Details
CVE-2026-49287	Statamic is a Laravel and Git powered content management system (CMS). Prior to 5.73.23 and 6.20.0, the fix for CVE-2026-41175 was incomplete. It addressed the issue in the query builder, but the same protection was not applied to in-memory collection sorting. Manipulating sort parameters could result in the loss of content and assets. This requires a front-end template that passes request input into a tag's sort parameter. It is not exploitable by default — a template would need to be explicitly set up to sort by a visitor-controlled value. This has been fixed in 5.73.23 and 6.20.0.	7.4	More Details
CVE-2026-3195	A flaw was found in QEMU. When reading input audio in the virtio-snd device input callback, the `virtio_snd_pcm_in_cb` function did not check whether the iov could fit the data buffer, potentially leading to a heap out-of-bounds write. This issue exists due to an incomplete fix for CVE-2024-7730.	7.4	More Details
CVE-2026-48505	Filament is a collection of full-stack components for accelerated Laravel development. From 4.0.0 until 4.11.5 and 5.6.5, a flaw in the handling of recovery codes for app-based multi-factor authentication allows the same recovery code to be reused via concurrent submission. This issue does not affect email-based MFA. It also only applies when recovery codes are enabled. If an attacker gains access to both the user's password and their recovery codes, they get two authenticated sessions per recovery code burned instead of one, or more if they batch the parallel submissions wider, materially extending the attacker's window of access compared to what the single-use guarantee implies. This vulnerability is fixed in 4.11.5 and 5.6.5.	7.4	More Details
CVE-2026-56815	pwnlift before d7a9544, in a privileged deployment, contains a symlink following vulnerability in the upload handler in Components/Pages/Home.razor.	7.4	More Details
CVE-2026-9006	IBM WebSphere Application Server 9.0, and 8.5 is vulnerable to server-side request forgery (SSRF) with the Ajax Proxy configured. This may allow an attacker to send unauthorized requests from the system, resulting in a security bypass or information disclosure.	7.4	More Details
CVE-2026-8646	IBM WebSphere Application Server 9.0 and 8.5 and IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.6 are vulnerable to HTTP request smuggling. A remote attacker could smuggle a specially crafted request to the application server thereby allowing the attacker to bypass security controls, spoof identity, escalate privilege, and expose sensitive information.	7.4	More Details
CVE-2026-12348	Address bar spoofing in Arc Search for Android allows a remote attacker to display a trusted domain in the address bar while rendering attacker-controlled content, enabling phishing.	7.4	More Details
CVE-2026-48294	Adobe Acrobat PDF Extension (Chrome) versions 26.5.2.2 and earlier are affected by a UXSS-class cross-origin data disclosure vulnerability. An attacker could exploit this vulnerability to gain access to data regarding the victim's session. Exploitation of this issue requires user interaction in that a victim must visit a maliciously crafted URL or interact with a compromised web page. Scope is changed.	7.4	More Details
CVE-2026-52698	Subscriber Sensitive Data Exposure in PushEngage – Web Push Notifications, eCommerce Automation & Chat Widget <= 4.2.3 versions.	7.4	More Details
CVE-2026-49502	Dell PowerFlex Manager, version(s) [Versions], contain(s) an Improper Authentication vulnerability. An unauthenticated attacker with adjacent network access could potentially exploit this vulnerability, leading to Information disclosure, Information tampering, and Unauthorized access.	7.4	More Details
	Impact: undici's ProxyAgent silently drops the requestTls option when configured with a SOCKS5		

CVE-2026-9697	proxy URI (socks5:// or socks://). The target HTTPS connection through the SOCKS5 tunnel falls back to Node's default trust store, ignoring user-configured ca, cert, key, rejectUnauthorized, and servername settings. Applications that pin to an internal or corporate CA via requestTls.ca will, when their proxy URI is SOCKS5, get the default Mozilla CA bundle as the trust anchor instead. Any cert signed by any publicly-trusted CA for the target hostname is accepted, breaking the intended pin and enabling MITM read and tamper of the HTTPS exchange. Affected applications are those that use undici's ProxyAgent (or Socks5ProxyAgent directly) with SOCKS5 AND rely on requestTls for TLS scope restriction. The bug was introduced in undici 7.23.0 when SOCKS5 support was added. Patches: Upgrade to undici v7.28.0 or v8.5.0. Workarounds: No workaround is available within the SOCKS5 path. If a SOCKS5 proxy with TLS scope restriction is required and an upgrade is not yet possible, route the traffic through an HTTP-proxy ProxyAgent instead, where requestTls is honored correctly.	7.4	More Details
CVE-2026-9029	The geomap panel's XYZ tile layer has a sanitize-then-interpolate ordering bug. sanitizeTextPanelContent() runs on the raw template string before getTemplateSrv().replace() substitutes the variable value, which uses the glob format with no HTML escaping. The result is passed to OpenLayers via element.innerHTML. An Editor can set a textbox variable's default value to an XSS payload that executes for every user who opens the dashboard. This is a bypass of the CVE-2023-0507 fix	7.3	More Details
CVE-2026-54328	Pi is a minimal terminal coding harness. From 0.74.0 until 0.78.1, Pi versions with temporary npm or git extension package installs used predictable paths under the operating system temporary directory. On Linux-based multi-user systems, a local attacker who can write to the shared temporary directory could prepare the expected package location before another user runs pi with a temporary extension package source. Pi could then load attacker-controlled extension code in the victim user's process. This vulnerability is fixed in 0.78.1.	7.3	More Details
CVE-2026-41046	A path traversal attack when using a "configName" parameter in qSnapper before version 1.3.3 allowed a local attacker to use malicious config files for snapper and so cause a denial of service or potentially escalate privileges to root.	7.3	More Details
CVE-2026-10845	IBM WebSphere Application Server 8.5 and 9.0 could allow a remote attacker to bypass authentication and gain unauthorized access to JAX-WS applications.	7.3	More Details
CVE-2026-12773	A weakness has been identified in BerriAI litellm up to 1.59.8. Affected is the function UserAPIKeyAuth of the file litellm/proxy/_experimental/mcp_server/auth/user_api_key_auth_mcp.py of the component MCP Proxy. Executing a manipulation can lead to improper authentication. The attack may 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.	7.3	More Details
CVE-2026-12530	Improper neutralization of argument delimiters in the install_packages() method in AWS Bedrock AgentCore Python SDK versions >= 1.1.3 and < 1.6.1 might allow a remote authenticated user to execute arbitrary commands within the Code Interpreter sandbox via crafted package name arguments. To mitigate this issue, users should upgrade to version 1.6.1.	7.3	More Details
CVE-2026-40768	Unauthenticated Insecure Direct Object References (IDOR) in Salon booking system <= 10.30.24 versions.	7.3	More Details
CVE-2026-49401	Deno is a JavaScript, TypeScript, and WebAssembly runtime. Prior to 2.7.14, Deno's permission system enforces filesystem and execution restrictions by comparing the requested path against the path supplied to --deny-read, --deny-write, --deny-run, or --deny-ffi. On macOS, that comparison was done at the raw-byte level while the APFS filesystem treats different Unicode spellings of the same name as the same file. That means a program could reach a denied path by spelling it differently than the deny rule. This vulnerability is fixed in 2.7.14.	7.3	More Details
CVE-2026-12529	A security vulnerability has been detected in SourceCodester CET Automated Grading System with AI Predictive Analytics 1.0. Affected is an unknown function of the file /index.php of the component Student Self-Registration Endpoint. The manipulation leads to improper access controls. Remote exploitation of the attack is possible.	7.3	More Details
	Vulnerability in the Oracle Access Manager product of Oracle Fusion Middleware (component: Web Server Plugin). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to		

CVE-2026-35314	compromise Oracle Access Manager. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Access Manager accessible data as well as unauthorized read access to a subset of Oracle Access Manager accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Access Manager. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L).	7.3	More Details
CVE-2025-69189	Missing Authorization vulnerability in EMV JobBank allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects JobBank: from n/a through 1.2.3.	7.3	More Details
CVE-2026-12775	A vulnerability was detected in Montodel House-Rental-Management up to 90010017b81265eb1ef3810268909f7719a33863. Affected by this issue is some unknown functionality of the file /login.php. The manipulation of the argument Username results in sql injection. The attack can be executed remotely. The exploit is now public and may be used. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2026-12795	A vulnerability was determined in BerriAI litellm up to 1.82.2. This affects the function json.dumps of the file litellm/proxy/management_endpoints/ui_sso.py of the component SSO Debug Flow. Executing a manipulation can lead to missing authentication. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure.	7.3	More Details
CVE-2026-46976	Vulnerability in the Oracle Public Sector Payroll product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Public Sector Payroll. Successful attacks of this vulnerability can result in takeover of Oracle Public Sector Payroll. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	7.2	More Details
CVE-2026-11407	Pimcore CMS/DXP version 12.3.8 contains a sandbox bypass vulnerability that allows authenticated administrative attackers to execute arbitrary methods on PHP objects by exploiting empty checkMethodAllowed() and checkPropertyAllowed() implementations in the custom Twig SecurityPolicy. Attackers can supply malicious Twig templates through the DataObject ClassDefinition Layout\Text component to perform arbitrary file reads, execute arbitrary database queries, and potentially achieve remote code execution via PHP object gadget chains, with the pimcore_* function wildcard further broadening the bypass to all Pimcore Twig functions.	7.2	More Details
CVE-2026-46969	Vulnerability in the Oracle Financials for EMEA product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Financials for EMEA. Successful attacks of this vulnerability can result in takeover of Oracle Financials for EMEA. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	7.2	More Details
CVE-2025-52465	GeoServer is an open source server that allows users to share and edit geospatial data. Prior to versions 2.26.4 and 2.27.3, a vulnerability exists that allows an authenticated administrator with access to GeoServer's security system to pass arbitrary file names to the Master Password Dump web page and create files containing the master password in plaintext. The provided file name must be an absolute path to the target file, the target file can not already exist and all parent directories must already exist. Versions 2.26.4 and 2.27.3 contain a fix. GeoServer installations where the web interface is either disabled or completely removed are not affected since the vulnerability exists in one of the web pages.	7.2	More Details
CVE-2025-27511	GeoServer is an open source server that allows users to share and edit geospatial data. Prior to version 2.27.0 of the GeoServer DB2 DataStore Extension, an administrator can perform a JNDI attack through specially crafted DB2 jdbc url leading to to Remote Code Execution (RCE). Version 2.27.0 fixes the issue.	7.2	More Details
CVE-2026-48895	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Apache APISIX. The attacker could manipulate some client headers to perform an open-redirect, to potentially expose the session token. This issue affects Apache APISIX: from 3.0.0 through 3.16.0. Users are	7.2	More Details

	recommended to upgrade to version 3.17.0, which fixes the issue.		
CVE-2026-46867	Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Extensibility Framework). Supported versions that are affected are 13.5 and 24.1. Easily exploitable vulnerability allows high privileged attacker with network access via HTTPS to compromise Oracle Enterprise Manager Base Platform. Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Manager Base Platform. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	7.2	More Details
CVE-2026-56382	Craft CMS (composer package craftcms/cms) versions >= 5.5.0 and <= 5.9.13 contain a remote code execution vulnerability in the FieldsController::actionRenderCardPreview() method, which passes the fieldLayoutConfig POST parameter directly to Fields::createLayout() without calling Component::cleanseConfig(). An authenticated admin user can inject Yii2 event handlers (e.g., 'on init' keys) via the fieldLayoutConfig parameter to execute arbitrary PHP code and disclose sensitive information (such as environment variables containing database credentials and CRAFT_SECURITY_KEY). The issue is fixed in version 5.9.14.	7.2	More Details
CVE-2026-46868	Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Extensibility Framework). Supported versions that are affected are 13.5 and 24.1. Easily exploitable vulnerability allows high privileged attacker with network access via HTTPS to compromise Oracle Enterprise Manager Base Platform. Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Manager Base Platform. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	7.2	More Details
CVE-2026-56446	MISP allowed a site administrator to configure an arbitrary filesystem path for the NDJSON error log used by JsonLogTool. Because log entries can include attacker-controlled content, an authenticated attacker with site administrator privileges could direct log output to a PHP file in a web-accessible directory and inject PHP code through logged data. Accessing the resulting file could lead to remote code execution with the privileges of the web server process. The fix restricts log destinations to existing directories beneath APP/tmp/logs or /var/log, requires absolute paths, rejects stream wrappers and traversal-related input, and limits filenames to .log or .ndjson extensions while disallowing executable extension segments.	7.2	More Details
CVE-2026-56447	MISP allowed an authenticated site administrator to set the Kafka_rdkafka_config setting to an arbitrary filesystem path. MISP subsequently parsed the referenced INI file and passed its options to rdkafka. A crafted attacker-controlled configuration file could use rdkafka options such as plugin.library.paths to load an external library, resulting in arbitrary code execution with the privileges of the MISP process. An attacker could leverage a MISP-writable location, such as an uploaded file or administrative image, to host the malicious configuration file. The issue is fixed by restricting the setting to absolute .ini files located only in approved configuration directories outside the webroot and MISP upload targets.	7.2	More Details
CVE-2026-46953	Vulnerability in the Oracle HRMS (UK) product of Oracle E-Business Suite (component: UK Payroll). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle HRMS (UK). Successful attacks of this vulnerability can result in takeover of Oracle HRMS (UK). CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	7.2	More Details
CVE-2026-46970	Vulnerability in the Oracle HR Intelligence product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle HR Intelligence. Successful attacks of this vulnerability can result in takeover of Oracle HR Intelligence. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	7.2	More Details
CVE-2026-46956	Vulnerability in the Oracle Property Manager product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Property Manager. Successful attacks of this vulnerability can result in takeover of Oracle Property Manager. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	7.2	More Details
	Vulnerability in the Oracle Project Portfolio Analysis product of Oracle E-Business Suite		

CVE-2026-46960	(component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Project Portfolio Analysis. Successful attacks of this vulnerability can result in takeover of Oracle Project Portfolio Analysis. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	7.2	More Details
CVE-2026-46938	Vulnerability in the Oracle Cost Management product of Oracle E-Business Suite (component: Cost Planning). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Cost Management. Successful attacks of this vulnerability can result in takeover of Oracle Cost Management. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	7.2	More Details
CVE-2026-46922	Vulnerability in the Oracle HR Intelligence product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle HR Intelligence. Successful attacks of this vulnerability can result in takeover of Oracle HR Intelligence. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	7.2	More Details
CVE-2026-10521	An high privileged remote attacker can access a hidden configuration method, that should not be accessible by any user, to modify critical program parameters. This can result in a total loss of confidentiality, integrity and availability.	7.2	More Details
CVE-2026-11409	An authenticated OS command injection vulnerability exists in the IPv6 PPPoE configuration handler in TL-WR940N v6 due to improper sanitization of user input. An attacker with administrative access may exploit this issue to execute arbitrary system commands with elevated privileges.	7.2	More Details
CVE-2026-35326	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Content. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	7.2	More Details
CVE-2026-56222	Capgo before 12.128.2 contains an authorization bypass vulnerability in POST /private/role_bindings that fails to verify app_id ownership during app-scoped role binding creation. An attacker with administrative privileges in one organization can create role bindings targeting applications owned by other organizations, enabling unauthorized read and modification of victim applications.	7.2	More Details
CVE-2026-44913	Improper escaping of database table names in the CaptureChangeMySQL Processor included with Apache NiFi 1.2.0 through 2.9.0 allows for injecting SQL commands using crafted naming. Manual quoted boundaries added in Apache NiFi 1.8.0 narrowed the scope of potential injection options, but did not cover additional strategies. Apache NiFi installations that do not use the CaptureChangeMySQL Processor are not subject to this vulnerability. Upgrading to Apache NiFi 2.10.0 is the recommended mitigation, which incorporates more robust identifier escaping.	7.2	More Details
CVE-2026-46769	Vulnerability in the Oracle Application Development Framework (ADF) product of Oracle Fusion Middleware (component: ADF Shared Components). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Application Development Framework (ADF). Successful attacks of this vulnerability can result in takeover of Oracle Application Development Framework (ADF). CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	7.2	More Details
CVE-2026-11410	An authenticated OS command injection vulnerability exists in the BigPond Cable (BPA) WAN configuration module in TL-WR940N v6 due to improper sanitization of user input. An attacker with administrative access may exploit this issue to execute arbitrary system commands with elevated privileges.	7.2	More Details
CVE-2026-	The CF7 to Webhook plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 5.0.0 via the pull_the_trigger. This makes it possible for unauthenticated attackers to make web requests to arbitrary locations originating from the web	7.2	More

11395	application and can be used to query and modify information from internal services. Exploitation requires that the admin-configured webhook URL contains a Contact Form 7 field placeholder in the host segment of the URL, and that the affected form is publicly accessible.		Details
CVE-2026-44914	Apache NiFi 1.12.0 through 2.9.0 are missing authorization when replacing Process Groups that include extension components with specific Required Permissions based on the Restricted annotation. The Restricted annotation indicates additional privileges required, but framework authorization did not check restricted status when handling requests to replace Process Groups. The missing authorization permits a user with general write access to add components with Restricted status. Apache NiFi installations that do not implement specific authorization for Restricted components are not subject to this vulnerability because the framework enforces write permissions as the security boundary. Upgrading to Apache NiFi 2.9.0 is the recommended mitigation, which removes the implementation of Restricted status authorization from the framework.	7.2	More Details
CVE-2025-69151	Unauthenticated Cross Site Scripting (XSS) in Grand Car Rental <= 3.7 versions.	7.1	More Details
CVE-2026-40720	Unauthenticated Cross Site Scripting (XSS) in Royal Elementor Addons Pro < 1.7.1041 versions.	7.1	More Details
CVE-2026-41557	Unauthenticated Cross Site Scripting (XSS) in Kapee < 1.7.1 versions.	7.1	More Details
CVE-2026-10651	A malformed Bluetooth Classic SDP attribute can trigger a reachable assertion in Zephyr's SDP parser. In subsys/bluetooth/host/classic/sdp.c, bt_sdp_parse_attribute() accepts an input buffer once it contains the 1-byte attribute type and 2-byte attribute id, but then unconditionally pulls an additional byte for the value type without verifying that the byte is present. A truncated 3-byte attribute (for example 09 00 09) therefore reaches net_buf_simple_pull() with insufficient remaining length, triggering the __ASSERT_NO_MSG(buf->len >= len) check and a kernel panic in assert-enabled builds (denial of service). In builds where assertions are disabled, parsing may continue past the end of the available buffer, leading to an out-of-bounds read and undefined behavior.	7.1	More Details
CVE-2026-10658	A missing length validation in the Zephyr Bluetooth Host ISO receive path can be triggered by malformed HCI ISO data. In bt_iso_recv() (subsys/bluetooth/host/iso.c), when processing PB=START/SINGLE fragments, the code pulls a TS SDU header (8 bytes, ts=1) or a non-TS SDU header (4 bytes, ts=0) without first verifying that buf->len contains at least that many bytes. The outer HCI ISO length check in hci_iso() validates payload length consistency but not the minimum inner SDU header size, so a packet with payload length 1 passes hci_iso() and then reaches net_buf_pull_mem(), which asserts buf->len >= len. As a result, malformed ISO traffic deterministically triggers a kernel assert (denial of service) in assert-enabled builds, and in non-assert builds the same path may proceed with an undersized buffer, leading to out-of-bounds read behavior. The issue affects products using the Zephyr Host with CONFIG_BT_ISO_RX enabled, particularly where incoming HCI data can be influenced by a malicious or compromised controller or malformed forwarded ISO traffic.	7.1	More Details
CVE-2026-56280	Cap-go before 12.128.2 contains a privilege inversion vulnerability in GET /build/logs/:jobId that allows read-only API key holders to cancel running native builds. The endpoint registers an abort listener on the SSE stream that unconditionally invokes cancelBuildOnDisconnect() using the privileged server-side BUILDER_API_KEY when clients disconnect, bypassing the app.build_native permission check required by the explicit POST /build/cancel/:jobId endpoint. Attackers with read-only API keys can repeatedly disrupt native build operations and CI/CD workflows by opening the log stream and dropping the connection.	7.1	More Details
CVE-2026-56314	Capgo before 12.128.12 fails to filter deleted app versions when joining channels during /updates resolution, allowing deleted bundles to remain selectable. Attackers can continue deploying deleted bundles to devices by exploiting the missing app_versions.deleted filter in channel version joins.	7.1	More Details
	TypeBot is a chatbot builder tool. Versions 3.15.2 and below have an Insecure Direct Object Reference vulnerability through cross-workspace Theme Template modification and deletion.		

CVE-2026-48759	The handleSaveThemeTemplate and handleDeleteThemeTemplate handlers validate that the authenticated user is a non-guest member of the provided workspaceId, but then operate on themeTemplateId via Prisma queries that do NOT include workspaceId in the WHERE clause. This allows any authenticated user to modify or delete theme templates belonging to any other workspace and may expose Template IDs via shared typebots or network traffic. This issue has been fixed in version 3.16.0.	7.1	More Details
CVE-2026-42385	Unauthenticated Cross Site Scripting (XSS) in Profile Builder Pro <= 3.15.0 versions.	7.1	More Details
CVE-2026-10641	Zephyr's Bluetooth Classic Hands-Free Profile (HFP) Hands-Free role parser (subsys/bluetooth/host/classic/hfp_hf.c) contains an out-of-bounds write. During Service Level Connection setup the HF sends AT+CIND=? and parses the AG's +CIND: response in cind_handle(), which assigns a per-entry counter index and calls cind_handle_values() for each list element. cind_handle_values() then wrote hf-ind_table[index] = i without verifying that index is within the 20-element int8_t ind_table[] array of struct bt_hfp_hf. Because the parser places no cap on the number of +CIND: list entries, a remote Attendant Gateway (a malicious, compromised, or spoofed peer the device connects to over Bluetooth) can send a response with more than 20 recognized indicator entries and drive index arbitrarily large, writing a small attacker-positioned value past the array into adjacent struct fields (feature masks, SDP/version state, the calls[] array, work/atomic bookkeeping) and potentially beyond the static connection pool slot. This yields memory corruption and at least denial of service of the Bluetooth host, triggered by a single malformed AT response with no user interaction. The sibling consumer ag_indicator_handle_values() already performed the equivalent bounds check; this commit adds the same index = ARRAY_SIZE(hf-ind_table) guard to close the gap. Affects builds with CONFIG_BT_HFP_HF enabled; introduced with the original HFP HF CIND parser (~v1.7) and present through v4.4.0.	7.1	More Details
CVE-2026-35066	Dell PowerFlex Manager, version(s) [Versions], contain(s) an Improper Access Control vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to denial of service.	7.1	More Details
CVE-2024-49269	Unauthenticated Cross Site Scripting (XSS) in my flatonica <= 0.0.8 versions.	7.1	More Details
CVE-2026-54290	Hono is a Web application framework that provides support for any JavaScript runtime. Prior to 4.12.25, with credentials: true and no explicit origin (the default wildcard), the CORS Middleware reflects the request's Origin and sends Access-Control-Allow-Credentials: true. Any site can then make credentialed cross-origin requests and read the responses, exposing cookie-authenticated endpoints to arbitrary origins. This vulnerability is fixed in 4.12.25.	7.1	More Details
CVE-2019-25749	Joomla J-CruisePortal 6.0.4 contains an SQL injection vulnerability that allows authenticated attackers to execute arbitrary SQL queries by injecting malicious code through the guest_adult parameter. Attackers can send POST requests to the cruises endpoint with crafted SQL payloads in the guest_adult parameter to extract sensitive database information or manipulate database records.	7.1	More Details
CVE-2026-22329	Unauthenticated Cross Site Scripting (XSS) in Skillate <= 1.2.10 versions.	7.1	More Details
CVE-2026-56209	An arbitrary address write vulnerability was found in libaom, the reference AV1 codec implementation. A missing bounds check in the SVC (Scalable Video Coding) layer ID control function allows an attacker to inject an arbitrary pointer into the cyclic refresh map field via crafted image pixel values. The encoder then writes approximately 1,200 bytes at the attacker-controlled address. This is fully deterministic and does not require a separate information leak. An attacker who can supply frames to a network-facing libaom encoder with SVC enabled could exploit this for denial of service or potential code execution.	7.1	More Details
CVE-2026-50146	Astro is a web framework. Prior to 6.3.3, when a component uses a client:* directive, Astro inserts named slot content into a data-astro-template attribute without HTML escaping the slot name allowing an attacker to break out of the attribute context and inject arbitrary HTML, resulting in reflected XSS during SSR. This vulnerability is fixed in 6.3.3.	7.1	More Details

CVE-2026-8172	The Simple Basic Contact Form WordPress plugin through 20250114 does not escape user-supplied input before reflecting it into the contact form output on validation errors, leading to a Reflected Cross-Site Scripting vulnerability that unauthenticated attackers can exploit against site visitors via a crafted link or cross-site form submission.	7.1	More Details
CVE-2025-69104	Unauthenticated Cross Site Scripting (XSS) in Qreatix <= 1.9.4 versions.	7.1	More Details
CVE-2025-59560	Unauthenticated Cross Site Scripting (XSS) in Sonaar <= 4.27.4 versions.	7.1	More Details
CVE-2025-31013	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themify Folo allows Reflected XSS. This issue affects Themify Folo: from n/a through 1.9.6.	7.1	More Details
CVE-2026-49346	libde265 is an open source implementation of the h.265 video codec. Prior to version 1.1.0, a crafted H.265 bitstream with large SPS dimensions and 16-bit bit depth causes a signed integer overflow in `de265_image_get_buffer()` (`libde265/image.cc:128`). The overflow wraps the plane allocation size to a small value (~1 KB), but the subsequent `fill_image()` call computes the real size using `size_t`, writing ~4 GB into the undersized heap buffer. Version 1.1.0 patches the issue.	7.1	More Details
CVE-2026-56211	A remote code execution vulnerability was found in libaom, the reference AV1 codec implementation. Insufficient bounds validation in the AV1 encoder's SVC (Scalable Video Coding) layer ID control allows an attacker to supply crafted video frame pixels that overlap with internal encoder layer context structures. In fork-based video processing services, an attacker can use this to hijack the cyclic refresh map pointer, brute-force the process base address via a crash oracle, and redirect control flow to achieve arbitrary command execution. Exploitation requires the target service to use libaom with SVC encoding enabled and accept attacker-supplied video frames.	7.1	More Details
CVE-2026-56210	A heap-buffer-overflow read vulnerability was found in libaom, the reference AV1 codec implementation. A missing bounds check in the SVC (Scalable Video Coding) layer ID control function allows setting a spatial_layer_id exceeding the configured number of layers. This causes an out-of-bounds heap read of approximately 40,728 bytes when computing a layer context array index. An attacker who can influence SVC encoder parameters in a network-facing service could exploit this for information disclosure (heap content leak) or denial of service (segmentation fault from hitting unmapped memory).	7.1	More Details
CVE-2026-22328	Unauthenticated Cross Site Scripting (XSS) in Auto Repair <= 22.6 versions.	7.1	More Details
CVE-2026-53915	In JetBrains GoLand before 2026.1.3 remote code execution was possible via untrusted project configuration	7.1	More Details
CVE-2026-48869	Unauthenticated Cross Site Scripting (XSS) in Enfold <= 7.1.4 versions.	7.1	More Details
CVE-2026-8089	The weMail: Email Marketing, Email Automation, Newsletters, Subscribers & Email Optins for WooCommerce WordPress plugin before 2.1.3 does not properly escape a user-supplied parameter before reflecting it into an HTML attribute on a non-nonce-protected AJAX response, allowing unauthenticated attackers to deliver Reflected Cross-Site Scripting against any authenticated user (including administrators) via a crafted URL.	7.1	More Details
CVE-2026-9570	The Taskbuilder WordPress plugin before 5.0.8 does not properly sanitise a URL parameter before echoing it into inline JavaScript on a frontend page containing one of its shortcodes, leading to a Reflected Cross-Site Scripting vulnerability that can be triggered against any logged-in user.	7.1	More Details
CVE-2026-	Unauthenticated Cross Site Scripting (XSS) in WPJobster <= 6.3.5 versions.	7.1	More Details

22339			
CVE-2026-54318	Home Assistant is open source home automation software that puts local control and privacy first. Prior to 2026.5.3, the LocationSensorManager BroadcastReceiver is exported with no permission. Any installed app, with zero runtime permissions, can broadcast a forged Google Play Services LocationResult directly to it; the receiver trusts the extra and forwards it to the user's Home Assistant server as the device's real location. This bypasses Android's developer-mode "Mock Location" gate and allows a local malicious app to drive zone-based automations (unlock door / disarm alarm / open garage) by faking the user's GPS position. This vulnerability is fixed in 2026.5.3.	7.1	More Details
CVE-2017-20265	Joomla! Component Flip Wall 8.0 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the wallid parameter. Attackers can send GET requests to index.php with the option=com_flipwall&task=click&wallid parameter containing SQL injection payloads to extract sensitive database information.	7.1	More Details
CVE-2017-20264	Joomla! Component Sponsor Wall 8.0 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the wallid parameter. Attackers can send GET requests to index.php with the option=com_sponsorwall&task=click&wallid parameter containing SQL injection payloads to extract sensitive database information including credentials and configuration data.	7.1	More Details
CVE-2026-4259	The ultimate-woocommerce-auction-pro WordPress plugin through 2.4.5 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	7.1	More Details
CVE-2025-68524	Unauthenticated Cross Site Scripting (XSS) in Avante < 3.0.5 versions.	7.1	More Details
CVE-2026-6858	The Transbank Webpay WordPress plugin before 1.14.0 does not sanitize and escape logs to be displayed, allowing unauthenticated users to perform Stored XSS attacks against logged in administrator	7.1	More Details
CVE-2025-69140	Unauthenticated Cross Site Scripting (XSS) in SweetDate Core < 1.1.5 versions.	7.1	More Details
CVE-2026-49778	Unauthenticated Cross Site Scripting (XSS) in WPFunnels Pro <= 2.9.4 versions.	7.1	More Details
CVE-2019-25761	Joomla! Component JoomCRM 1.1.1 contains an SQL injection vulnerability that allows authenticated attackers to execute arbitrary SQL queries by injecting malicious code through the deal_id parameter. Attackers can send GET requests to index.php with option=com_joomcrm&view=contacts and inject SQL code in the deal_id parameter to extract sensitive database information including table names and schemas.	7.1	More Details
CVE-2026-49074	Unauthenticated Cross Site Scripting (XSS) in JetEngine <= 3.8.9.1 versions.	7.1	More Details
CVE-2026-40765	Unauthenticated Cross Site Scripting (XSS) in collectchat <= 2.4.9 versions.	7.1	More Details
CVE-2026-49338	gonic is a music streaming server / free-software subsonic server API implementation. Prior to version 0.21.0, the Subsonic API endpoints `/rest/deletePlaylist.view` and `/rest/getPlaylist.view` perform no per-resource authorization. Once authenticated as any user (admin or not), an attacker can delete any playlist owned by any other user (including admin) by passing its `id` and read the full contents (name, comment, song list) of any other user's **private** (non-public) playlist by passing its `id`. The Subsonic playlist `id` is `base64url("<userID>/<filename>.m3u")`. Because filenames are user-supplied or time-derived and the `userID` is a small integer, IDs are guessable and frequently exposed (e.g. a previously-public playlist that was later made private still has the same ID). This breaks the multi-user trust	7.1	More Details

	boundary of gonic: a low-privileged user can wipe an administrator's curated playlists, and a user can exfiltrate any private playlist they obtain an ID for. The issue was fixed in commit `6dd71e6a3c966867ef8c900d359a7df75789f410`, which is part of version 0.21.0.		
CVE-2026-48997	e107 is a content management system (CMS). Versions 2.3.5 and earlier contain a command injection vulnerability in the ImageMagick resize destination path. In resize_image(), the source path is escaped with escapeshellarg(), but the destination path is inserted inside raw double quotes in the convert command; in the submit-news upload flow, that destination filename includes the first six characters of user-controlled news title input. Because the title filter removes literal spaces but not tab characters, and shell expansions such as $(...) and backticks can survive into the quoted destination argument, /bin/sh -c may evaluate attacker-controlled input. Exploitation is possible only when all of the following non-default settings are enabled: resize_method=ImageMagick, subnews_attach=1, upload_enabled=1, subnews_resize is numeric between 30 and 5000, and the attacker is a non-admin in classes permitted by both subnews_class and upload_class. This issue has been fixed in version 2.3.6.	7.1	More Details
CVE-2026-49339	gonic is a music streaming server / free-software subsonic server API implementation. The maintainer's fix in commit `6dd71e6a3c966867ef8c900d359a7df75789f410` added an ownership check based on `playlist.UserID`. However, `playlist.UserID` is derived from the first path segment of the attacker-controlled playlist ID, with no path containment on the resolved file path. Any authenticated Subsonic user can therefore bypass the ownership check and read any other user's playlist, delete any other user's playlist, and probe arbitrary file paths on the host for existence/readability. This is a bypass of the boundary the `6dd71e6` fix is trying to enforce; it is closely related to the original GONIC-1 IDOR but uses a different primitive (path traversal in the `id` parameter rather than direct cross-user access). Commit 0824bed88f6bbc490ba28bf09d28e5dfeb07b445 in version 0.21.0 fixes the issue.	7.1	More Details
CVE-2026-54195	Unauthenticated Cross Site Scripting (XSS) in JetFormBuilder <= 3.6.0.1 versions.	7.1	More Details
CVE-2026-54192	Unauthenticated Cross Site Scripting (XSS) in Popup box <= 6.2.9 versions.	7.1	More Details
CVE-2026-46932	Vulnerability in the Oracle Enterprise Asset Management product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Enterprise Asset Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Enterprise Asset Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Enterprise Asset Management. CVSS 3.1 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L).	7.1	More Details
CVE-2019-25757	Joomla vWishlist 1.0.1 contains an SQL injection vulnerability that allows authenticated attackers to execute arbitrary SQL queries by injecting malicious code through the vproductid and userid parameters. Attackers can send POST requests to the component with crafted SQL payloads in these parameters to extract sensitive database information including version and database names.	7.1	More Details
CVE-2026-46914	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Filesystem). The supported version that is affected is 11.4. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Solaris accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Solaris. CVSS 3.1 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H).	7.1	More Details
CVE-2019-25759	Joomla! Component vBizz 1.0.7 contains an SQL injection vulnerability that allows authenticated attackers to execute arbitrary SQL queries by injecting malicious code through the payid parameter. Attackers can submit POST requests to the employee management interface with crafted payid array values containing SQL commands to extract sensitive database information including version and database names.	7.1	More Details
CVE-			

2026-39548	Unauthenticated Cross Site Scripting (XSS) in MagOne <= 9.0 versions.	7.1	More Details
CVE-2026-49295	libde265 is an open source implementation of the h.265 video codec. Prior to version 1.0.20, a crafted H.265 bitstream can cause an out-of-bounds array write in `decoder_context::process_reference_picture_set()` (`libde265/decctx.cc:1376`). The root cause is a missing aggregate bound check on predicted short-term reference picture set entries. Individual list sizes are validated, but the combined count after predicted RPS construction can exceed the 16-entry `PocStFoll` array, writing at index 16. Version 1.0.20 patches the issue.	7.1	More Details
CVE-2026-54012	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.6, Open WebUI lets a user who can create, update, or import workspace models store arbitrary meta.knowledge entries on their model without checking whether they own or can read the referenced files. Open WebUI then treats meta.knowledge entries of type file as an authorization source in two places: the built-in view_file tool reads the file's extracted text, and has_access_to_file()'s model branch authorizes the file content and file delete endpoints. A malicious model owner can therefore attach another user's file ID to their model metadata and read or delete that private file. This vulnerability is fixed in 0.9.6.	7.1	More Details
CVE-2026-54189	Unauthenticated Cross Site Scripting (XSS) in JetEngine <= 3.8.10 versions.	7.1	More Details
CVE-2026-54188	Unauthenticated Cross Site Scripting (XSS) in JetEngine <= 3.8.10 versions.	7.1	More Details
CVE-2026-39597	Unauthenticated Cross Site Scripting (XSS) in WPZOOM Addons for Elementor <= 1.3.4 versions.	7.1	More Details
CVE-2026-54321	Daytona is a secure and elastic infrastructure runtime for AI-generated code execution and agent workflows. From 0.101.0 until 0.184.0, sandbox previews that were switched from public to private could remain reachable without authentication for a short period after the change, due to a cached visibility state that was not invalidated when the sandbox's visibility changed. This vulnerability is fixed in 0.184.0.	7.0	More Details
CVE-2026-0083	In Nfc::eventCallback() of Nfc.h, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.0	More Details
CVE-2026-56404	libexpat before 2.8.2 has an integer overflow in addBinding.	6.9	More Details
CVE-2026-56403	libexpat before 2.8.2 has an integer overflow in storeAtts.	6.9	More Details
CVE-2026-56406	libexpat before 2.8.2 has an integer overflow in XML_ParseBuffer because it lacked a check that was present in XML_Parse.	6.9	More Details
CVE-2026-56407	libexpat before 2.8.2 has an integer overflow in doProlog that is related to storeEntityValue and entity textLen.	6.9	More Details
CVE-2026-56408	libexpat before 2.8.2 has an integer overflow in copyString.	6.9	More Details
CVE-2026-56132	In libexpat before 2.8.2, there is a heap-based buffer overflow in doProlog in xmlparse.c because scaffold backing array reallocation is mishandled when there is data-structure sharing across parsers.	6.9	More Details
CVE-			

2026-56410	xmlwf in libexpat before 2.8.2 has an integer overflow in resolveSystemId.	6.9	More Details
CVE-2026-56405	libexpat before 2.8.2 has an integer overflow in getAttributeId.	6.9	More Details
CVE-2026-56411	xmlwf in libexpat before 2.8.2 has an integer overflow in endDoctypeDecl via NOTATION declarations.	6.9	More Details
CVE-2026-47693	Poweradmin is a web-based DNS administration tool for PowerDNS server. Versions prior to 4.2.4 and 4.3.3 are vulnerable to CSV Injection (Formula Injection) in its log export functionality. User-controlled data — specifically the username field — is written to exported CSV files without sanitizing formula trigger characters (=, +, -, @). When an administrator exports activity logs and opens the resulting CSV in a spreadsheet application (Microsoft Excel, LibreOffice Calc, Google Sheets), any formula stored in a username is executed by the application. This can be used for phishing attacks against administrators or data exfiltration. Versions 4.2.4 and 4.3.3 patch the issue.	6.9	More Details
CVE-2026-56109	The Advanced Linux Sound Architecture (ALSA) library before 1.2.16.1 contains a double-free vulnerability in parse_def() in src/conf.c that allows attackers to corrupt memory by supplying maliciously crafted ALSA configuration text. When parsing nested compound or array configuration blocks, parse_def() fails to check return values before continuing, causing snd_config_delete() to be called twice on the same already-freed node, resulting in a NULL-pointer write or invalid memory read.	6.8	More Details
CVE-2026-7842	The Infility Global Infility Global WordPress plugin before 2.15.20 for WordPress does not sanitize or validate the orderby and order parameters in the import_list(), url_detail(), and file_detail() admin page callbacks before using them in SQL queries, allowing authenticated attackers with Editor-level access or higher to perform time-based blind SQL injection and extract sensitive data from the database. The ImportData module must be enabled via the Infility Global WordPress plugin before 2.15.20's module toggle page.	6.8	More Details
CVE-2026-10609	A missing authorization flaw was found in the OpenShift Cluster Logging Operator. The operator creates and forwards ServiceAccount tokens to output destinations without verifying that the ClusterLogForwarder creator has permission to use those credentials, allowing a delegated editor to exfiltrate SA tokens and escalate privileges.	6.8	More Details
CVE-2026-48117	DroneAware is a drone detection platform. The centralized DroneAware server backing droneaware.io was vulnerable to an account pre-hijacking attack in which an attacker could register an account using a victim's email address with an attacker-controlled password before the victim completed account activation. When the legitimate owner later activated the account, either by clicking the email verification link or by logging in via Google SSO, the attacker-set password became fully valid, enabling silent and persistent account takeover without any notification to the victim. The vulnerability was fixed server-side on 2025-05-20; no user action is required. Node binaries and self-hosted detection nodes are not affected. There are no workarounds; the fix was deployed server-side and no client-side mitigation is applicable.	6.8	More Details
CVE-2026-54196	Subscriber Privilege Escalation in JetFormBuilder <= 3.6.1 versions.	6.8	More Details
CVE-2026-48782	Pydantic AI is a Python agent framework for building applications and workflows with Generative AI. In versions 1.56.0 through 1.101.0, 2.0.0b1, and 2.0.0b2, the cloud-metadata blocklist could be bypassed by encoding the metadata IP in an IPv6 transition form that the previous fix, CVE-2026-46678, did not decode, exposing cloud IAM short-term credentials. The previous remediation decoded only IPv4-mapped IPv6, 6to4, and the NAT64 well-known prefix, so the metadata guarantee did not hold for the remaining transition forms: IPv4-compatible IPv6 (::a.b.c.d), the NAT64 RFC 8215 local-use prefix (64:ff9b:1::/48), operator-chosen NAT64 prefixes, and ISATAP. The IPv6 wrapper is then delivered to the underlying IPv4 metadata endpoint. This occurs when an application using Pydantic AI opts a URL into force_download='allow-local' (which disables the default block on private/internal IPs) and runs on a network that actually routes the affected IPv6 transition forms: NAT64-configured networks (IPv6-only or dual-stack-with-NAT64 deployments, including some Kubernetes setups) for the	6.8	More Details

	NAT64 variants, or networks with an ISATAP tunnel for ISATAP. A standard dual-stack cloud VM or container does not route these forms and is not affected in practice. The IPv4-compatible and Teredo variants are deprecated and addressed as defense-in-depth. This is an incomplete fix of GHSA-cqp8-fcvh-x7r3 / CVE-2026-46678 (itself a follow-up to CVE-2026-25580). This issue has been fixed in version 2.0.0b3.		
CVE-2026-56342	AVideo through version 27.0 contains a server-side request forgery vulnerability in plugin/Live/test.php that allows authenticated administrators to read arbitrary URLs via the statsURL parameter, which lacks isSSRFSafeURL() validation and accepts requests to private IP ranges and cloud metadata endpoints. Attackers can exploit this by crafting requests to internal services, cloud metadata endpoints like 169.254.169.254, and localhost to retrieve sensitive information including IAM credentials, internal service responses, and network configuration details.	6.8	More Details
CVE-2026-55201	Evil-WinRM through 3.9, fixed in commit 6ecd570, contains a path traversal vulnerability in the download_dir() function that allows a rogue or compromised remote Windows server to write files outside the intended download directory by returning filenames with traversal sequences from Get-ChildItem command output that are passed unsanitized to File.join(). Attackers controlling the remote server can exploit this to overwrite sensitive client-side files such as SSH authorized_keys or shell configuration files, achieving persistent access or privilege escalation on the client machine.	6.8	More Details
CVE-2026-48981	pam_usb provides hardware authentication for Linux using ordinary removable media. In versions prior to 0.9.2, pam_usb calls xmlReadFile() with flags=0 when loading the configuration file, allowing libxml2 to process external entity references (XXE), potentially making outbound network connections or local file reads at XML parse time from the context of the authenticating process. The vulnerability requires the configuration file to contain crafted XML entity references. Since pam_usb.conf is root-owned, direct exploitation requires prior write access to the config, but the defence-in-depth impact is significant given that pam_usb.so runs in setuid contexts (sudo, su). This issue has been fixed in version 0.9.2.	6.7	More Details
CVE-2026-12115	The Counter Box – Add Countdowns, Timers & Dynamic Counters to WordPress plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 2.0.13 via deserialization of untrusted input . This makes it possible for authenticated attackers, with administrator-level access and above, to inject a PHP Object. No known POP chain is present in the vulnerable software, which means this vulnerability has no impact unless another plugin or theme containing a POP chain is installed on the site. If a POP chain is present via an additional plugin or theme installed on the target system, it may allow the attacker to perform actions like delete arbitrary files, retrieve sensitive data, or execute code depending on the POP chain present. Deserialization is triggered automatically upon the post-import redirect that renders the list table, and again when any item is opened for editing, requiring no additional navigation beyond the import action itself.	6.6	More Details
CVE-2026-35291	Vulnerability in the WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 14.1.2.0.0 and 15.1.1.0.0. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise WebLogic Server. Successful attacks of this vulnerability can result in takeover of WebLogic Server. CVSS 3.1 Base Score 6.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H).	6.6	More Details
CVE-2026-46869	Vulnerability in the MySQL Shell product of Oracle MySQL (component: Shell: Dump and Load). Supported versions that are affected are 8.4.0-8.4.9 and 9.0.0-9.7.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Shell. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Shell accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N).	6.5	More Details
CVE-2026-32682	When NGINX Gateway Fabric is configured using GRPCRoutes, an authenticated, remote attacker with permission to create or modify GRPCRoute resources can cause the NGINX Gateway Fabric control plane to terminate by sending undisclosed GRPCRoute configurations containing backendRef filters. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	6.5	More Details
	GeoServer is an open source server that allows users to share and edit geospatial data. Prior to		

CVE-2025-58175	versions 2.26.4 and 2.27.3, a GeoServer that uses `ENTITY_RESOLUTION_ALLOWLIST` may allow attacker to perform unauthenticated Server-Side Request Forgery (SSRF). This vulnerability requires that GeoServer is set up to use a proxy base URL and the `ENTITY_RESOLUTION_ALLOWLIST` (default since 2.25.0). Versions 2.26.4 and 2.27.3 contain a fix. GeoServer installations are only affected by this vulnerability if they use a proxy base URL that does not contain a URL path or end with a slash. If the proxy base URL does not contain a path, adding a slash to the end of the URL will mitigate this vulnerability.	6.5	More Details
CVE-2026-54009	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.6, POST /api/chat/completions accepts an image_url.url value that, when it does NOT start with http://, https://, or data:image/, is interpreted as a file id and resolved against the global file table with no ownership check. an authenticated user can therefore set image_url.url to another user's file id, the server reads that file from disk, base64-encodes it, and injects the data URI into the LLM request. the user then prompts the LLM to describe / OCR the file and reads the content back. This vulnerability is fixed in 0.9.6.	6.5	More Details
CVE-2026-55198	Hermes WebUI before 0.51.443 contains an authorization bypass vulnerability in the session export endpoint that allows authenticated users to access sessions from other profiles. The _handle_session_export handler in api/routes.py fails to verify active-profile ownership before serializing session data, enabling attackers to exfiltrate foreign session transcripts by guessing or knowing session identifiers.	6.5	More Details
CVE-2026-22551	In Eclipse Theia versions prior to 1.71.0, the AI chat rendered Markdown image tags from AI responses, triggering HTTP requests to arbitrary external URLs without restriction. Combined with prompt injection in a malicious workspace, an attacker could induce the AI agent to construct image URLs encoding sensitive information from the workspace or conversation context, exfiltrating it to attacker-controlled servers. The workspace trust enforcement introduced in v1.71.0 mitigates the documented attack chain by disabling AI features in untrusted workspaces.	6.5	More Details
CVE-2026-48129	Kestra is an open-source, event-driven orchestration platform. Prior to versions 1.3.19, 1.2.19, 1.1.19, and 1.0.43, Kestra task `inputFiles` writes rendered file names directly under the task working directory. When a flow forwards untrusted execution or webhook data into an `inputFiles` file name, a caller can use `../` path segments to create or overwrite files outside that task working directory on the worker filesystem. Versions 1.3.19, 1.2.19, 1.1.19, and 1.0.43 patch the issue.	6.5	More Details
CVE-2026-46871	Vulnerability in the MySQL Shell product of Oracle MySQL (component: Shell for VS Code). The supported version that is affected is 2026.2.0+9.6.1. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Shell. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Shell accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	6.5	More Details
CVE-2026-49411	Deno is a JavaScript, TypeScript, and WebAssembly runtime. Prior to 2.8.0, the Node.js compatibility TCP path checked the permission against the original hostname string before resolution and then did not re-check after resolution. A caller could therefore pass a numeric alias of an IP address (for example the decimal integer 2130706433 or the hex form 0x7f000001, both of which resolve to 127.0.0.1) and reach the denied destination through node:net.connect or node:http.request's { host, port } options form. This vulnerability is fixed in 2.8.0.	6.5	More Details
CVE-2025-71382	MuPDF before 1.27.0-rc1 contains an uncontrolled recursion vulnerability in the EPUB CSS rendering engine that allows remote attackers to cause a denial of service by supplying a maliciously crafted EPUB file with deeply nested HTML elements and inline CSS styles. The function value_from_inheritable_property() in css-apply.c recurses through the CSS property inheritance chain without a depth limit, exhausting the process stack and causing a crash in any application using MuPDF for EPUB rendering.	6.5	More Details
CVE-2026-56116	dhcpcd through 10.3.2, fixed in commit 708b4a5, contains a memory leak vulnerability in the IPv6 Router Advertisement route information handling that allows an unauthenticated same-link attacker to cause denial of service by sending crafted Router Advertisements. Attackers can repeatedly send Router Advertisements containing Route Information options with a lifetime of zero, triggering unfreed allocations in routeinfo_findalloc() that cause linear memory exhaustion and eventual daemon crash.	6.5	More Details

CVE-2026-49133	Typemill before 2.24.0 contains a path traversal vulnerability that allows authenticated attackers with Author-level privileges to read arbitrary files outside the content directory by supplying traversal sequences in the path query parameter passed to Storage::getFile() with an empty folder argument. Attackers can bypass traversal-prevention controls in Storage::getFolderPath() to access sensitive files.	6.5	More Details
CVE-2024-51454	IBM Engineering Workflow Management 7.0.2 through 7.0.2 Interim Fix 035, 7.0.3 through 7.0.3 Interim Fix 017, and 7.1 through 7.1 Interim Fix 004 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-2026-49072	Unauthenticated Broken Access Control in WooCommerce Anti-Fraud <= 7.2.6 versions.	6.5	More Details
CVE-2026-42357	Incorrect Authorization vulnerability allows users to access workflow instance information belonging to projects they do not have permission to access. This issue affects Apache DolphinScheduler versions prior to 3.4.2. Users are recommended to upgrade to version 3.4.2, which fixes this issue.	6.5	More Details
CVE-2026-55197	Hermes WebUI before 0.51.443 contains a broken access control vulnerability in the /api/session endpoint that allows authenticated users to disclose cross-profile session transcripts. Attackers can bypass profile boundary checks by directly querying session IDs belonging to other profiles via GET /api/session?session_id=<foreign_id>&messages=1 to retrieve unauthorized conversation transcripts and metadata.	6.5	More Details
CVE-2026-46810	Vulnerability in the Identity Manager product of Oracle Fusion Middleware (component: End User Self Service). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP to compromise Identity Manager. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Identity Manager accessible data as well as unauthorized read access to a subset of Identity Manager accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).	6.5	More Details
CVE-2026-54019	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.6, Open WebUI added collection-level ACL checks, but the patch can still be bypassed when Milvus multitenancy mode is enabled. The ACL allows unknown non-KB collection names as legacy/ephemeral collections. In Milvus multitenancy mode, that user-controlled collection name becomes a resource_id and is interpolated into a Milvus expression without escaping. This is caused by an incomplete fix for CVE-2026-44560 This vulnerability is fixed in 0.9.6.	6.5	More Details
CVE-2026-56346	AVideo through version 25.0 contains an authentication bypass vulnerability in the decryptMessage.json.php endpoint that allows unauthenticated users to decrypt PGP messages. Remote attackers can submit private keys, ciphertext, and passphrases to perform server-side decryption without credentials, exposing key material to logs and enabling resource exhaustion attacks.	6.5	More Details
CVE-2026-56409	xmlwf in libexpat before 2.8.2 has an integer overflow for the output filename when -d outputDir is used.	6.5	More Details
CVE-2026-47277	Runtipi is a personal homeserver orchestrator. In versions 4.9.1 through 4.9.3, Runtipi serves marketplace app logos from files inside cloned app-store repositories through an unauthenticated endpoint, which leads to arbitrary file read through app-store logo symlinks. The path guard checks only the lexical path before Node reads the file, so a Git app store that contains metadata/logo.jpg as a symbolic link can cause Runtipi to read and return the symlink target. Because the endpoint is public and the symlink target may point outside the cloned repository, this can expose local files from the Runtipi container such as /data/.env, /data/state/seed, logs, or application files. This can disclose JWT secrets, service credentials, local configuration, and operational logs depending on the instance. The issue has been fixed in version 4.10.0.	6.5	More Details

CVE-2026-54518	jackson-databind contains the general-purpose data-binding functionality and tree-model for Jackson Data Processor. From 2.21.0 until 2.21.4 and 3.1.4, UnwrappedPropertyHandler.processUnwrappedCreatorProperties() replays buffered JSON into creator parameters but never consults prop.visibleInView(activeView). The normal property-based creator path gates creator properties on the active view, but this unwrapped-creator replay path bypasses that check, so a constructor parameter annotated with both @JsonView(AdminView.class) and @JsonUnwrapped is populated from attacker JSON even when a more restrictive view is active. This vulnerability is fixed in 2.21.4 and 3.1.4.	6.5	More Details
CVE-2026-49359	PhpWeasyPrint is a PHP library allowing PDF generation from a URL or an HTML page. Prior to version 2.6.0, `pontedilana/php-weasyprint` fetches the content of option values server-side via `file_get_contents()` when the value looks like a URL, without restricting the URL scheme. The `attachment` option of `Pdf` is the reachable sink: any value that passes `isOptionUrl()` (`filter_var(..., FILTER_VALIDATE_URL)`) is downloaded by the PHP process and embedded into the generated PDF. Because `FILTER_VALIDATE_URL` accepts `http`, `https`, `ftp`, `file` and PHP stream wrappers such as `php://`, an attacker who can influence the `attachment` value reaches both a **Server-Side Request Forgery** primitive (e.g. internal HTTP endpoints, cloud metadata) and a local file disclosure primitive (`file://`, `php://filter/...`), with the fetched bytes exfiltrated as a PDF attachment. This is the same class of issue KnpLabs/snappy patched for its `xsl-style-sheet` option in GHSA-c5fp-p67m-gq56. The library is documented as a one-to-one substitute for KnpLabs/snappy and shares the same code shape. PhpWeasyPrint version 2.6.0 contains a patch for the issue.	6.5	More Details
CVE-2026-35261	Vulnerability in the Oracle Access Manager product of Oracle Fusion Middleware (component: Authentication Engine). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Access Manager. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Access Manager accessible data as well as unauthorized read access to a subset of Oracle Access Manager accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).	6.5	More Details
CVE-2026-45436	Subscriber Broken Access Control in WPBakery Page Builder <= 8.7.2 versions.	6.5	More Details
CVE-2026-9815	The MagicForm WordPress plugin through 0.1.3 does not properly validate the type of files uploaded through an unauthenticated AJAX action when a form's per-field extension allowlist is left empty, allowing unauthenticated attackers to upload PHP files and execute arbitrary code on the server.	6.5	More Details
CVE-2026-56304	picklescan before 1.0.1 contains an unsafe pickle deserialization vulnerability allowing unauthenticated attackers to create arbitrary zero-byte files via logging.FileHandler class instantiation. Attackers can exploit this by crafting malicious pickle payloads to bypass RCE blocklists and create lock files or other filesystem artifacts, potentially causing denial of service or application disruption.	6.5	More Details
CVE-2026-49271	libheif is a HEIF and AVIF file format decoder and encoder. Prior to version 1.22.1, the uncompressed HEIF decoder validates explicit icef compressed-unit offsets using unit_offset + unit_size. Because the addition can wrap, a crafted HEIF file can pass the range check and then construct a vector from iterators outside the compressed item buffer, producing an out-of-bounds heap read and crash. Version 1.22.1 patches the issue.	6.5	More Details
CVE-2026-27878	A TraceQL query in Grafana Tempo with a large exemplars hint value can cause the Tempo instance to allocate an excessive amount of memory, resulting in an out-of-memory crash. This could allow an authenticated user to trigger a denial of service against the Tempo service.	6.5	More Details
CVE-2026-46551	NocoDB is software for building databases as spreadsheets. Prior to 2026.04.4, the uploadViaURL path in the v1/v2 attachment API did not enforce NC_ATTACHMENT_FIELD_SIZE against the remote content-length or against the response stream. An authenticated user (Editor+) could direct the server to download arbitrarily large files, exhausting disk space and causing denial of service. In packages/nocodb/src/services/attachments.service.ts, the HEAD probe read content-length but never compared it to NC_ATTACHMENT_FIELD_SIZE; the subsequent storageAdapter.fileCreateByUrl() performed the download without maxContentLength. This vulnerability is fixed in 2026.04.4.	6.5	More Details

CVE-2026-11820	Module: plugins/modules/nexmo.py CVSS 3.1: 6.5 MEDIUM — AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N Issue: api_key and api_secret are declared no_log=True at the input level, but both credentials are immediately URL-encoded into a GET request as query parameters, bypassing all no_log protection. Vulnerable Code (lines 82-93): msg = { "api_key": module.params.get("api_key"), "api_secret": module.params.get("api_secret"), "from": module.params.get("src"), "text": module.params.get("msg"), } url = f"{NEXMO_API}? {urlencode(msg)}" response, info = fetch_url(module, url, headers=headers) Observed Output: https://rest.nexmo.com/sms/json? api_key=a1b2c3d4&api_secret=MyS3cr3tK3y!!&from=AnsibleBot&to=15551234567&text=Hello Exposure Vectors: Ansible verbose output (-vvv) logs the full request URL Vonage/Nexmo server access logs record credentials in query string HTTP proxies, SIEM, and network inspection tools capture the full URL AWX/Automation Controller network debug logs Fix: Switch to POST with credentials in the request body: data = urlencode({"api_key": api_key, "api_secret": api_secret, "from": src, "to": number, "text": msg}) fetch_url(module, NEXMO_API, data=data, method="POST", headers={"Content-Type": "application/x-www-form-urlencoded"})	6.5	More Details
CVE-2026-54324	Daytona is a secure and elastic infrastructure runtime for AI-generated code execution and agent workflows. Prior to 0.185.0, a cross-tenant authorization flaw in Daytona's notification WebSocket gateway allowed any authenticated user to subscribe to another organization's realtime notification channel and passively receive that organization's events. This vulnerability is fixed in 0.185.0.	6.5	More Details
CVE-2026-42490	[This CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] To create and manage guests, domctl operations are used by the control domain, a possible Xenstore domain, or by a domain controlling a particular guest. Some of these operations may not be executed in parallel, so a system-wide lock is used. The way that lock is acquired is, however, not providing any fairness. This is CVE-2026-42489. Furthermore, with XSM/Flask in use, the lock acquire will, for some operations, occur ahead of any permission checking. This is CVE-2026-42490.	6.5	More Details
CVE-2026-47340	Allow authenticated users to access alert instances associated with alert groups they do not have permission to access. in Apache DolphinScheduler. This issue affects Apache DolphinScheduler: before 3.4.2. Users are recommended to upgrade to version 3.4.2, which fixes the issue.	6.5	More Details
CVE-2026-40724	CP Client Arbitrary File Download in Client Portal (Pro) <= 5.6.2 versions.	6.5	More Details
CVE-2024-54178	IBM Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data versions 4.8,5.0,5.1,5.2,5.3 could allow an authenticated user to cause a denial of service when creating new databases due to improper allocation of resources.	6.5	More Details
CVE-2026-44942	A path traversal in handling the "path" component of .repo files processed by libzypp before 17.38.13 in the 17.x series, or before 16.22.19 could be used by attackers to fill directories on the system outside of the zypp cache with content.	6.5	More Details
CVE-2026-12119	The Simple File List plugin for WordPress is vulnerable to unauthorized file operations due to a missing authorization check on the 'frontmanage' shortcode attribute in all versions up to, and including, 6.3.7. This makes it possible for authenticated attackers, with contributor-level access and above, to perform arbitrary file operations including deletion, move, folder creation, and download. An attacker can create a draft post containing the 'eeSFL' shortcode, render it via the post preview endpoint to harvest the nonce needed to authorize the operations, and then submit file operation requests that bypass the intended authorization checks in includes/ee-list-ops-bar-process.php.	6.5	More Details
CVE-2026-39433	Subscriber Arbitrary Content Deletion in WPAMS < 49.5.3 versions.	6.5	More Details
CVE-2026-27410	Unauthenticated Deserialization of untrusted data in Slimstat Analytics < 5.4.0 versions.	6.5	More Details
CVE-	Craft CMS from 4.0.0-RC1 contains an authenticated path traversal vulnerability in the assets/icon endpoint where the extension parameter is not validated before file existence		More

2026-56394	checks. Attackers can bypass extension validation by passing traversal sequences that resolve to existing SVG files, allowing local file read access.	6.5	Details
CVE-2026-54817	Authentication Bypass Using an Alternate Path or Channel vulnerability in FluxBuilder MStore API allows Password Recovery Exploitation. This issue affects MStore API: from n/a through 4.18.4.	6.5	More Details
CVE-2026-48067	Filament is a collection of full-stack components for accelerated Laravel development. From filament/actions 4.0.0 until 4.11.4 and 5.6.4 and from filament/tables 3.0.0 until 3.3.51, the recordSelectOptionsQuery() method may be used to scope the options available in the Select field for AttachAction and AssociateAction. However, the built-in validation rule for these fields did not apply the same scope. As a result, a user who can trigger these actions could tamper with the Livewire component's state and submit an out-of-scope value. This vulnerability is fixed in filament/actions 4.11.4 and 5.6.4 and filament/tables 3.3.51.	6.5	More Details
CVE-2026-8118	The Royal Addons for Elementor – Addons and Templates Kit for Elementor plugin for WordPress is vulnerable to Arbitrary File Read in versions 1.7.1058 through 1.7.1059. This is due to the wpr_get_csv_handle() helper (introduced in version 1.7.1058 as part of the patch for CVE-2026-6229) falling back to is_readable() and fopen($source, 'r') on the attacker-controlled settings.table_upload_csv.url value when it does not parse as an HTTP URL, with no allow-list, traversal block, or extension check. This makes it possible for authenticated attackers, with Contributor-level access and above, to save a crafted wpr-data-table widget through Elementor's save_builder endpoint and have the rendered preview return the line-by-line contents of any file readable by the PHP process, including wp-config.php.	6.5	More Details
CVE-2025-15661	libssh2 through 1.11.1, fixed in commit 2dae302, contains an out-of-bounds heap read vulnerability in the sftp_symlink() function in src/sftp.c that allows a malicious SSH server or man-in-the-middle attacker to disclose heap memory contents or cause a crash by sending a crafted SSH_FXP_NAME response. Attackers can supply a link_len value larger than the actual packet data in SSH_FXP_NAME responses for SFTP READLINK and REALPATH operations, triggering a heap buffer over-read of up to target_len minus one bytes due to the missing validation of available packet buffer size before the memcpy operation.	6.5	More Details
CVE-2026-50519	Initialization of a resource with an insecure default in GitHub Copilot and Visual Studio Code allows an unauthorized attacker to disclose information over a network.	6.5	More Details
CVE-2026-48500	Filament is a collection of full-stack components for accelerated Laravel development. From 3.0.0 until 3.3.52, 4.11.5, and 5.6.5, any schema can contain a file upload form field, so Filament applies Livewire's WithFileUploads trait to the Livewire component the schema is embedded in. However, some schemas, such as the panel login form, do not require file uploads, and exposing unauthenticated temporary file uploads on these components is not an acceptable risk. On these components, an unauthenticated attacker could upload arbitrary files to the application's temporary storage, which could be abused to exhaust disk space or inflate storage costs. This vulnerability is fixed in 3.3.52, 4.11.5, and 5.6.5.	6.5	More Details
CVE-2025-69137	Subscriber Broken Access Control in Genemy <= 1.6.6 versions.	6.5	More Details
CVE-2026-56229	Capgo before 12.128.2 contains an authorization bypass vulnerability in the /build/status and /build/logs endpoints that allows attackers to access build jobs belonging to different applications by supplying a mismatched app_id and job_id combination. Limited API keys restricted to a single app can retrieve build status and logs from other apps by providing an authorized app_id while using a job_id from an unauthorized app, exposing sensitive build information including logs, metadata, and potentially credentials.	6.5	More Details
CVE-2026-12450	Inappropriate implementation in Media in Google Chrome prior to 149.0.7827.155 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	6.5	More Details
CVE-	phpMyFAQ is an open source FAQ web application. Versions prior to 4.1.4 have Missing Authorization in the API CategoryController. CVE-2026-24421 addressed this in the BackupController by adding: $this->userHasPermission(PermissionType::BACKUP). The same fix was not applied to 4 other write endpoints in the public API. All 4 only call $this-		

2026-49205	>hasValidToken() — which checks a shared API key header, rather than the individual user's role permissions. The following APIs are affected: POST /api/v4.0/category (CategoryController::create), POST /api/v4.0/faq (FaqController::create), PUT /api/v4.0/faq (FaqController::update), and POST /api/v4.0/question (QuestionController::create). This issue has been fixed in version 4.1.4.	6.5	More Details
CVE-2026-11989	The Bit integrations – Form Integration, Webhook, Spreadsheets, CRM, LMS & Email Automation plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 2.8.7 via the upload_attachment. 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. Exploitation requires a form integration to be configured with a field mapped to a WooCommerce product image, product gallery, downloadable files, or Google Contacts attachment field, which is a default use case for these integrations.	6.5	More Details
CVE-2026-54233	vLLM is an inference and serving engine for large language models (LLMs). Prior to 0.23.1rc0, vLLM's /v1/audio/transcriptions endpoint limits compressed upload size but not decoded PCM output. A 25MB OPUS file expands to ~14.9GB of float32 PCM at decode time. This vulnerability is fixed in 0.23.1rc0.	6.5	More Details
CVE-2026-54911	UltraJSON is a fast JSON encoder and decoder written in pure C with bindings for Python 3.7+. Prior to 5.13.0, ujson.dumps() (or ujson.dump() or ujson.encode()) have a reject_bytes=False option. When set, they may accept malformed or truncated UTF-8 byte sequences, silently rewriting them into different Unicode characters instead of rejecting them. This leads to input validation bypass and data integrity issues. This vulnerability is fixed in 5.13.0.	6.5	More Details
CVE-2026-56221	Cap-go before 12.128.2 contains multiple SQL injection vulnerabilities in cloudflare.ts where user-controlled values from API request bodies are interpolated directly into SQL query strings without sanitization or parameterization. Authenticated users with read-level API key permissions can inject arbitrary SQL through deviceIds, search, version_name, cursor, and actions parameters to access analytics data belonging to other users or applications.	6.5	More Details
CVE-2026-44645	LiquidJS is a Shopify/GitHub Pages compatible template engine written in pure JavaScript. In versions 10.25.7 and below, the renderLimit option can be fully bypassed by a {% for %} (or {% tablerow %}) tag whose body is empty. The renderLimit option is documented in docs/source/tutorials/dos.md as the mechanism that "mitigates this by limiting the time consumed by each render() call." The per-iteration time check is reached only when the body contains at least one template node, so a template such as {%- for i in (1..N) -%}{%- endfor -%} iterates the full collection without ever consulting renderLimit. With a configured renderLimit of 50 ms, a single parseAndRenderSync call has been observed to consume 2.26 seconds (~45× over the limit) and scales linearly with N up to memoryLimit, allowing a low-privileged template author to wedge an event-loop thread for an attacker-chosen duration. Deployments that rely on a finite renderLimit for DoS protection (common in multi-tenant template-authoring environments) can still be forced by a single crafted template to monopolize a Node.js event-loop worker for attacker-controlled time, potentially stalling in-flight requests, with availability impact only. This issue has been fixed in version 10.26.0.	6.5	More Details
CVE-2026-50201	Steeltoe is an open source project that provides a collection of libraries that helps users build cloud-native applications. In Steeltoe.Management.Endpoint prior to version 4.2.0 and Steeltoe.Management.EndpointCore prior to version 3.4.0, all Steeltoe actuator endpoints default to `EndpointPermissions.Restricted`, which is mappeds to Cloud Foundry's `read_basic_data` permission (granted to Space Auditors and similar low-trust roles). Sensitive actuators including heap dump, environment, and thread dump do not raise this to `EndpointPermissions.Full`, so CF's `read_sensitive_data` permission flag is not enforced for those endpoints. Spring Boot's equivalent Cloud Foundry integration gates these endpoints with `read_sensitive_data` by default. Steeltoe.Management.Endpoint 4.2.0 and Steeltoe.Management.EndpointCore 3.4.0 patch the issue. If an immediate upgrade is not possible, explicitly set `RequiredPermissions = EndpointPermissions.Full` in the options for `HeapDumpEndpointOptions`, `EnvironmentEndpointOptions`, and `ThreadDumpEndpointOptions`; and/or if heap dump, thread dump, or environment are not needed in production, register only the required actuators individually instead of using `AddAllActuators()`.	6.5	More Details
CVE-	Dell PowerFlex Manager, versions prior to 4.5.1.1, contain an improper certificate validation		More

2024-47477	vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability leading to man-in-the-middle attack in tandem with DNS cache poisoning.	6.5	Details
CVE-2026-56077	PraisonAI before 1.5.115 contains an information disclosure vulnerability in the MultiAgentLedger component that allows attackers to access sensitive data by registering agents with duplicate IDs. Attackers can exploit the lack of agent ID uniqueness enforcement to share ledger instances and expose system prompts and conversation history between agents.	6.5	More Details
CVE-2026-52866	An attacker within BLE communication range can monopolize the device's only available BLE connection slot, preventing legitimate users or applications from establishing a connection.	6.5	More Details
CVE-2026-50034	An attacker within BLE communication range can passively intercept wireless traffic and obtain sensitive health-related information, including glucose measurement values.	6.5	More Details
CVE-2026-9822	The WP Hotel Booking WordPress plugin before 2.3.1 does not enforce capability checks in several of its AJAX handlers, allowing authenticated users with Subscriber-level access to read other users' booking line items, enumerate active coupons, and read pricing data.	6.5	More Details
CVE-2026-42895	Improper neutralization of special elements used in a command ('command injection') in Microsoft Copilot allows an unauthorized attacker to perform tampering over a network.	6.5	More Details
CVE-2026-42867	Langflow is a tool for building and deploying AI-powered agents and workflows. Prior to 1.9.0, Langflow is vulnerable to Path Traversal in the Knowledge Bases API (POST /api/v1/knowledge_bases). This occurs because user-supplied knowledge base names are used directly to create file paths without proper sanitization or containment checks. An authenticated attacker can exploit this flaw to create directories and write files anywhere on the server's filesystem. This vulnerability is fixed in 1.9.0.	6.5	More Details
CVE-2026-12568	The postman_download module uses the workspace name field from the Postman API to construct the local directory path without sanitization. If a malicious workspace has a name containing path traversal characters, pathlib resolves the path outside the intended output directory, allowing an attacker to write arbitrary files to the user's system.	6.5	More Details
CVE-2026-56024	Cross-Site Request Forgery (CSRF) vulnerability in Saad Iqbal WP EasyPay allows Cross Site Request Forgery. This issue affects WP EasyPay: from n/a through 4.4.0.	6.5	More Details
CVE-2026-47155	vLLM is an inference and serving engine for large language models (LLMs). Prior to 0.22.0, vLLM's revision pinning controls do not consistently apply to all artifacts loaded for a model. A deployment that supplies --revision or --code-revision can still load dynamic code, GGUF files, image processors, retrieval side weights, or same-repository subfolder weights/config from an unpinned/default revision. This is a supply-chain integrity issue for pinned vLLM deployments. Operators can believe they are serving a reviewed model revision while vLLM resolves behavior-affecting nested or sibling artifacts outside that reviewed revision. This vulnerability is fixed in 0.22.0.	6.5	More Details
CVE-2026-46979	Vulnerability in the PeopleSoft Enterprise CS Campus Community product of Oracle PeopleSoft (component: Integration and Interfaces). The supported version that is affected is 9.2.38. Easily exploitable vulnerability allows high privileged attacker with network access via HTTPS to compromise PeopleSoft Enterprise CS Campus Community. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all PeopleSoft Enterprise CS Campus Community accessible data as well as unauthorized access to critical data or complete access to all PeopleSoft Enterprise CS Campus Community accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N).	6.5	More Details
CVE-2026-56695	OpenHarness ohmo gateway /resume and /summary slash commands default remote_invocable to True, allowing admitted remote senders to enumerate and load arbitrary session snapshots by ID. Attackers can exploit this to access victim snapshots containing private prompts, credentials, tool output, and file paths via shared gateway channels.	6.5	More Details
CVE-	NanoClaw before 2.1.17 contains a privilege escalation vulnerability in the handleApprovalsResponse function that fails to verify responder role authorization. Attackers		More

2026-56402	with a valid questionId can approve or reject privileged actions like package installation by submitting approval response payloads without proper role validation.	6.5	Details
CVE-2026-48140	There is an unchecked enum cast vulnerability in NI grpc-device BeginSidebandStream that may allow an attacker to trigger invalid enum states and undefined behavior, potentially resulting in a denial of service. Successful exploitation requires an attacker to supply a specially crafted message containing an out-of-range value. This affects NI grpc-device 2.17.0 and prior versions.	6.5	More Details
CVE-2026-56079	Capgo before 12.128.2 contains a cross-tenant authorization bypass vulnerability in PostgREST endpoints that allows org-scoped read API keys to access other tenants' webhook secrets and delivery logs. Attackers can query the webhooks and webhook_deliveries endpoints to exfiltrate HMAC signing secrets and delivery payloads, enabling forged webhook events against victim organizations.	6.5	More Details
CVE-2026-52673	SQL Injection vulnerability in Cboard v.0.4.2 and before allows a remote attacker to execute arbitrary code via the getDimensionsValues component	6.5	More Details
CVE-2026-47341	Authentication Bypass by Capture-replay vulnerability in Apache APISIX. Attacker can benefit from certain configurations in hmac-auth to re-use a token forever, bypassing expiry. This issue affects Apache APISIX: from 3.11.0 through 3.16.0. Users are recommended to upgrade to version 3.17.0, which fixes the issue.	6.5	More Details
CVE-2025-55639	GPAC MP4Box v2.4 was discovered to contain a NULL pointer dereference in the gf_isom_add_track_kind() function at isomedia/isom_write.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted MP4 file.	6.5	More Details
CVE-2026-56701	Grav before 2.0.0-beta.2 contains an XML external entity injection vulnerability in SVG file upload processing that allows authenticated attackers to read arbitrary files. The application uses simplexml_load_string without disabling external entity loading, enabling attackers to inject XXE payloads via malicious SVG files to exfiltrate sensitive data.	6.5	More Details
CVE-2024-35690	Insertion of sensitive information into sent data vulnerability in MarketingFire Widget Options allows Retrieve Embedded Sensitive Data. This issue affects Widget Options: from n/a through 4.0.1.	6.5	More Details
CVE-2024-37210	Missing Authorization vulnerability in ali2woo AliNext allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects AliNext: from n/a through 3.3.5.	6.5	More Details
CVE-2026-54288	Hono is a Web application framework that provides support for any JavaScript runtime. Prior to 4.12.25, the Body Limit Middleware trusts the request's Content-Length header to decide whether a body is within the limit. On AWS Lambda (API Gateway v1/v2, ALB, VPC Lattice, and Lambda@Edge) the body is delivered fully buffered and the adapter builds the request with the client-declared Content-Length, which need not match the actual payload. A client can declare a tiny Content-Length while sending a much larger body, slipping past the limit. This vulnerability is fixed in 4.12.25.	6.5	More Details
CVE-2026-12706	A use-after-free vulnerability was found in FFmpeg's RASC video decoder. The decode_move() function initializes a read pointer into a decompressed buffer, but a subsequent reallocation of that same buffer during move-table processing leaves the pointer dangling. An attacker could exploit this by providing a specially crafted AVI file containing a malicious RASC video stream. When a user opens or plays the file, the decoder reads from freed heap memory, which could lead to a denial of service (crash).	6.5	More Details
CVE-2026-12461	Out of bounds read in WebRTC in Google Chrome on Windows prior to 149.0.7827.155 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	6.5	More Details
CVE-2026-52716	Unauthenticated Arbitrary File Deletion in WorkScout-Core <= 1.7.11 versions.	6.5	More Details
CVE-	Gophish through 0.12.1 contains a denial of service vulnerability that allows authenticated users with the User role to exhaust server memory by uploading a crafted Office document as an email template attachment. The ApplyTemplate() function in models/attachment.go processes		More

2026-39904	Office documents as ZIP archives and calls ioutil.ReadAll() on each contained file entry without enforcing size restrictions on uncompressed content, allowing a zip bomb payload to expand to several gigabytes in memory and cause the process to be terminated by the operating system.	6.5	Details
CVE-2026-49071	Unauthenticated Broken Authentication in WooCommerce Dropshipping <= 5.2.4 versions.	6.5	More Details
CVE-2026-56251	Capgo before 12.128.2 contains a broken row level security policy in the org_users table that allows authenticated users to elevate privileges from admin to super_admin. Attackers can exploit the insufficient RLS enforcement to gain unauthorized super_admin access and compromise system security.	6.5	More Details
CVE-2026-12136	The Customize My Account For Woocommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'sysbasics_user_avatar' shortcode in versions up to, and including, 4.3.6. This is due to insufficient input sanitization and output escaping on user supplied attributes (min_height, min_width, max_height, max_width) in the wcmamtx_get_avatar_default() function, which are concatenated unescaped into the get_avatar() extra_attr style 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-2026-1856	The Appointment Booking Calendar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via custom booking field labels in all versions up to, and including, 1.4.4 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-2026-8607	The Points Management System For Gamification, Ranks, Badges, and Loyalty Rewards Program – myCred plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'wrap' Shortcode Attribute in all versions up to, and including, 3.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-4328	The Advanced Import plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 1.4.6. This is due to the plugin using wp_remote_get() to fetch a user-supplied URL without validating that the URL does not point to internal or private network resources in the demo_download_and_unzip() function. The 'demo_file' parameter from $_POST is passed through sanitize_text_field() (which only handles XSS-related sanitization) and then directly into wp_remote_get() when 'demo_file_type' is set to 'url'. Notably, the plugin uses wp_safe_remote_get() in other locations (theme template libraries) which would provide SSRF protection, but fails to use it in this critical AJAX handler. This makes it possible for authenticated attackers, with Author-level access and above (upload_files capability), to make web requests to arbitrary locations originating from the web application, which can be used to query and view data from internal services, including cloud instance metadata endpoints.	6.4	More Details
CVE-2026-12157	The BetterDocs - Knowledge Base Docs & FAQ Solution for Elementor & Block Editor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the blockId attribute of the betterdocs/category-slate-layout Gutenberg block in versions up to, and including, 4.5.3. This is due to insufficient input sanitization and output escaping in the CategorySlateLayout::render() method, which echoes the blockId block attribute directly into an HTML class attribute without esc_attr(). This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-56306	Capgo before 12.128.2 contains a weak parsing vulnerability in the x-limited-key-id header that allows attackers to bypass subkey enforcement by submitting malformed values, zero, or duplicate headers that result in NaN or falsy values. Remote attackers can manipulate the x-limited-key-id header to disable limited key scoping and execute requests using the main API key context instead of restricted subkey permissions.	6.4	More Details
CVE-2026-	Mattermost versions 11.7.x <= 11.7.0, 11.6.x <= 11.6.2, 11.5.x <= 11.5.5, 10.11.x <= 10.11.17 fail to authenticate Atlassian Connect installed callbacks, allowing a remote	6.4	More

6673	unauthenticated attacker to inject a rogue sharedSecret and disrupt the Jira integration via POST to /ac/installed during the pending-install window.. Mattermost Advisory ID: MMSA-2026-00654		Details
CVE-2026-4610	The ProfileGrid – User Profiles, Groups and Communities plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'pm_author_message' parameter in the pm_send_message_to_author function in all versions up to, and including, 5.9.9.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The vulnerability was partially patched in version 5.9.8.5.	6.4	More Details
CVE-2026-6062	Mattermost versions 11.7.x <= 11.7.0, 11.6.x <= 11.6.2, 11.5.x <= 11.5.5, 10.11.x <= 10.11.17 Fail to validate channel ownership of an existing subscription before applying edits which allows an authenticated attacker to hijack subscriptions from channels they have no access to via a crafted PUT request to the subscription edit endpoint.. Mattermost Advisory ID: MMSA-2026-00650	6.4	More Details
CVE-2026-8494	The Permalink Manager Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via post titles in the admin URI Editor interface in all versions up to, and including, 2.5.3.3 due to insufficient output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in the admin Permalink Manager page that will execute whenever an administrator accesses the Permalink Manager page.	6.4	More Details
CVE-2026-48167	Filament is a collection of full-stack components for accelerated Laravel development. From 4.0.0 until 4.11.5 and 5.6.5, the ImageColumn and ImageEntry components render raw database values without escaping HTML. Where the data passed to these components isn't validated, an attacker could plant malicious HTML or JavaScript and achieve stored XSS that executes for users who view the table or schema. This vulnerability is fixed in 4.11.5 and 5.6.5.	6.4	More Details
CVE-2026-11402	The Services Section Block – Showcase Service Details in Grid or Columns plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'link' Block Attribute in all versions up to, and including, 1.4.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The payload persists inside HTML comments in post_content, bypassing wp_kses_post sanitization at save time, and executes via both the primary service link anchor and a secondary title-wrapped anchor when the linkIn option is set to 'title'.	6.4	More Details
CVE-2026-54015	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.6, Open WebUI's prompt version-history endpoints authorize the prompt_id in the URL but then act on caller-supplied history IDs without verifying that the history row belongs to that prompt (history_entry.prompt_id == prompt.id). This affects /api/v1/prompts/id/{prompt_id}/history/diff, /api/v1/prompts/id/{prompt_id}/update/version, and /api/v1/prompts/id/{prompt_id}/history/{history_id}. An authenticated user with access to any prompt they control, plus a victim prompt_history.id, can read or delete another user's private prompt history. This vulnerability is fixed in 0.9.6.	6.4	More Details
CVE-2026-8039	The Fancy Testimonials plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'author' shortcode attribute in the 'testimonial' shortcode in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-2021	The Slideshow Gallery LITE plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'alwaysauto' shortcode attribute in all versions up to, and including, 1.8.5. This is due to insufficient input sanitization and output escaping on user-supplied attributes. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2026-12098	The PowerPress Podcasting plugin by Blubrry plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'embed' Episode Meta Field in all versions up to, and including, 11.16.8 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The embed value is stored via update_post_meta() rather than through WordPress core's post content pipeline, meaning kses-	6.4	More Details

	on-save filtering is never applied — even for Author-role users who would otherwise lack unfiltered_html — making this path unprotected by WordPress's standard role-based XSS mitigations.		
CVE-2026-12808	A vulnerability was determined in Edimax BR-6478AC V2 1.23. This impacts the function stainfo of the file /goform/stainfo of the component POST Request Handler. This manipulation of the argument interface causes command injection. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-48980	pam_usb provides hardware authentication for Linux using removable media. In versions prior to 0.9.2, getenv() environment variables XRDP_SESSION, DISPLAY and TMUX allow environment variable injection into local-check logic. These environment variables influence whether a current session is local or remote, and a PAM module that runs in the context of setuid binaries (sudo, su), getenv() returns attacker-controlled values whenever the process environment has been manipulated by a local user. This issue has been fixed in version 0.9.2.	6.3	More Details
CVE-2026-54021	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.6, several direct, index-addressed Ollama proxy routes accept a caller-supplied url_idx path parameter and use it as a raw index into the admin-configured OLLAMA_BASE_URLS list. Access control on these routes validates only whether the user may use the requested model, never which backend the request is routed to. Any authenticated user can append an arbitrary url_idx to force their request onto an Ollama backend they were never authorized to reach, including internal, higher-privilege, or explicitly admin-disabled backends. This vulnerability is fixed in 0.9.6.	6.3	More Details
CVE-2026-55249	@rtk-ai/rtk-rewrite transparently rewrites shell commands executed via OpenClaw's exec tool to their RTK equivalents. In 1.0.0, the @rtk-ai/rtk-rewrite OpenClaw plugin passes attacker-controlled input directly into a shell-backed execSync() template string without shell-safe escaping. JSON.stringify() wraps the value in double quotes and escapes inner double-quotes and backslashes, but leaves $() and backtick shell metacharacters untouched. Because execSync delegates execution to /bin/sh -c, the shell expands $(...) substitutions even inside double-quoted strings, causing the injected subcommand to execute before rtk is invoked. An attacker who can influence the exec tool's command parameter (e.g., via an LLM agent prompt or gateway/tool-call input) achieves arbitrary OS command execution with the privileges of the plugin/gateway process.	6.3	More Details
CVE-2026-12774	A security vulnerability has been detected in BerriAI litellm up to 1.82.2. Affected by this vulnerability is the function _execute_with_mcp_client of the file litellm/proxy/_experimental/mcp_server/rest_endpoints.py of the component MCP Server Connection Testing. The manipulation leads to server-side request forgery. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure.	6.3	More Details
CVE-2026-12726	A flaw was found in the AWX GitHub webhook integration. When processing GitHub pull_request webhooks, the controller stores the pull_request.statuses_url value from the webhook payload without validating that it points to a trusted GitHub API endpoint. If a job template is configured with a GitHub Personal Access Token as its webhook credential, the controller later POSTs that token to the stored callback URL when posting job status updates. An attacker who can submit a correctly signed forged webhook using the job template's webhook_key can redirect the callback to an attacker-controlled URL and exfiltrate the configured GitHub PAT.	6.3	More Details
CVE-2026-12772	A security flaw has been discovered in BerriAI litellm up to 1.82.2. This impacts the function authenticate_user of the file litellm/proxy/auth/login_utils.py of the component PROXY_ADMIN database API Key Generator. Performing a manipulation results in session expiration. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure.	6.3	More Details
CVE-2026-12807	A vulnerability was found in Edimax BR-6478AC V2 1.23. This affects the function setWAN of the file /goform/setWAN of the component POST Request Handler. The manipulation of the argument pppUserName/pptpUserName/L2TPUserName results in command injection. It is possible to launch the attack remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-	Capgo before 12.128.2 contains an authorization bypass vulnerability in webhook management endpoints that allows non-expiring API keys to bypass the require_apikey_expiration		

2026-56295	organization policy. The checkWebhookPermission function fails to call apikeyHasOrgRightWithPolicy, enabling attackers with legacy non-expiring keys to list, create, and delete webhooks despite explicit organizational policy requiring key expiration.	6.3	More Details
CVE-2026-12821	A vulnerability was determined in FlowiseAI Flowise up to 3.1.2. The impacted element is an unknown function of the file packages/components/nodes/documentloaders/S3/S3.ts of the component S3 Document Loader. Executing a manipulation can lead to path traversal. It is possible to launch the attack remotely. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-12805	A flaw has been found in OFFIS DCMTK up to 3.7.0. The affected element is the function XMLNode::parseFile in the library ofstd/libsrc/ofxml.cc. Executing a manipulation can lead to heap-based buffer overflow. The attack may be performed from remote. The exploit has been published and may be used. This patch is called 1d4b3815c0987840a983160bfc671fef63a3105b. It is best practice to apply a patch to resolve this issue. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.	6.3	More Details
CVE-2026-12809	A vulnerability was identified in Edimax BR-6478AC V2 1.23. Affected is the function wiz_5in1_redirect of the file /goform/wiz_5in1_redirect of the component POST Request Handler. Such manipulation of the argument newpass leads to command injection. The attack can be launched remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-12810	A security flaw has been discovered in Edimax BR-6478AC V2 1.23. Affected by this vulnerability is the function mp of the file /goform/mp of the component POST Request Handler. Performing a manipulation of the argument command results in command injection. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-12813	A vulnerability was detected in activepieces up to 0.83.0. This vulnerability affects the function handleUrlFile in the library packages/server/engine/src/lib/variables/processors/file.ts of the component File URL Handler. The manipulation results in server-side request forgery. The attack can be executed 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.	6.3	More Details
CVE-2026-12814	A flaw has been found in Comfast CF-WR631AX V3 up to 2.7.0.8. This issue affects the function system of the file /cgi-bin/mbox-config?section=ping_config of the component API Endpoint. This manipulation of the argument destination causes os command injection. The attack is possible to be carried out remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-20220	A vulnerability in the web-based management interface of Cisco Crosswork Network Controller could allow an authenticated, remote attacker to execute arbitrary commands on an affected device. This vulnerability is due to insufficient input validation in the configuration template engine of the web-based management interface. An attacker could exploit this vulnerability by sending a crafted request to the affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system in limited areas of the file system. This vulnerability affects only areas of the operating system for which the template user has write permissions. To exploit this vulnerability, the attacker must have valid template user credentials with write permissions. Template users with read permissions cannot exploit this vulnerability.	6.3	More Details
CVE-2026-12787	A vulnerability was found in zhilink 智互联(深圳)科技有限公司 ADP Application Developer Platform 应用开发者平台 1.0.0. This affects an unknown part of the component testConnection Endpoint. The manipulation of the argument jdbcUrl results in deserialization. The attack may be performed from remote. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-12815	A vulnerability has been found in coollabsio coolify 4.0.0. Impacted is an unknown function of the component Image Name Handler. Such manipulation leads to os command injection. The attack may be performed from remote. The vendor was contacted early about this disclosure but did not respond in any way. The changelog for 4.1.2 mentions "[i]mproved image, branch, proxy, and deployment input validation".	6.3	More Details

CVE-2026-44911	Authorization handling for component configuration verification requests in Apache NiFi 1.15.0 through 2.9.0 allows clients with read access to submit proposed configuration properties. The proposed properties override current configuration, enabling users with read access to invoke predefined verification methods with alternative settings. Apache NiFi installations that do not implement different levels of authorization for viewing and modifying component configuration are not subject to this vulnerability. Upgrading to Apache NiFi 2.10.0 is the recommended mitigation, requiring write access to submit configuration verification requests.	6.3	More Details
CVE-2026-21768	The compose-rich-editor library (v1.0.0-rc14) used in HCL Verse for Android's rich text email composition fails to properly validate all HTML input thereby allowing malicious content to be executed in certain situations.	6.3	More Details
CVE-2026-12798	A weakness has been identified in BerriAI litellm up to 1.82.2. Affected by this vulnerability is the function load_openapi_spec_async of the file litellm/proxy/_experimental/mcp_server/openapi_to_mcp_generator.py of the component MCP OpenAPI Spec Loader. This manipulation of the argument spec_path causes server-side request forgery. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure.	6.3	More Details
CVE-2026-12797	A security flaw has been discovered in BerriAI litellm up to 1.82.5. Affected is the function async_pre_call_hook of the file enterprise/enterprise_hooks/banned_keywords.py of the component Completions Interface. The manipulation of the argument prompt results in incorrect authorization. The attack may be performed from remote. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure.	6.3	More Details
CVE-2026-12796	A vulnerability was identified in BerriAI litellm up to 1.82.2. This impacts the function get_redirect_response_from_openid of the file litellm/proxy/management_endpoints/ui_sso.py of the component SSO Authentication Flow. The manipulation leads to session expiration. The attack is possible to be carried out remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure.	6.3	More Details
CVE-2026-12788	A vulnerability was determined in zhilink 智互联(深圳)科技有限公司 ADP Application Developer Platform 应用开发者平台 1.0.0. This vulnerability affects unknown code of the file /adpweb/a/base/barcodeDetail/import of the component XML Parser. This manipulation causes xml external entity reference. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2026-12776	A flaw has been found in Montodel House-Rental-Management up to 90010017b81265eb1ef3810268909f7719a33863. This affects an unknown part of the file /index.php?page=houses. This manipulation of the argument ID 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.	6.3	More Details
CVE-2019-25760	Joomla! Component Easy Shop 1.2.3 contains a local file inclusion vulnerability that allows unauthenticated attackers to read arbitrary files by supplying base64-encoded file paths. Attackers can send GET requests to index.php with the option parameter set to com_easyshop, task set to ajax.loadImage, and a base64-encoded file path in the file parameter to retrieve sensitive files like configuration.php and system files.	6.2	More Details
CVE-2026-9073	A flaw was found in foreman-mcp-server. This component utilizes two distinct logging mechanisms that can expose sensitive session and authentication data. One mechanism logs session identifiers, which are treated as authentication credentials, at an informational level. The other, when debug logging is enabled, incompletely sanitizes HTTP request headers, leading to the cleartext logging of sensitive information such as authorization tokens and API keys. This vulnerability can result in a confidentiality breach, as sensitive authentication data is persisted in plain text within container logs, increasing the risk if logs are forwarded to a centralized platform.	6.2	More Details
CVE-2026-56347	AVideo TopMenu plugin through version 26.0 contains a stored cross-site scripting vulnerability in menu item rendering due to missing output encoding of icon classes, URLs, and text labels. Attackers can inject malicious JavaScript through unescaped menu item fields that execute for all site visitors, potentially stealing session cookies or performing unauthorized actions.	6.1	More Details

CVE-2026-56317	Nuxt before 4.4.7 (and the 3.x branch before 3.21.7) contains a cross-site scripting vulnerability in the NoScript component that writes slot content to innerHTML without escaping. Attackers can inject malicious scripts through untrusted data in NoScript slots, such as route.query parameters, which execute in the document context when the noscript tag is implicitly closed by script tags.	6.1	More Details
CVE-2026-44915	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Apache APISIX. The default configuration of cas-auth in Apache APISIX is vulnerable to phishing and credential theft. This issue affects Apache APISIX: from 3.0.0 through 3.16.0. Users are recommended to upgrade to version 3.17.0, which fixes the issue.	6.1	More Details
CVE-2026-56236	Capgo CLI before 12.128.2 contains arbitrary file overwrite vulnerabilities in login and build credentials operations that follow symlinks without validation. Attackers can create malicious symlinks in repositories to overwrite arbitrary files or expose credentials with world-readable permissions when developers run the CLI.	6.1	More Details
CVE-2026-12459	Inappropriate implementation in Serial in Google Chrome prior to 149.0.7827.155 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: High)	6.1	More Details
CVE-2026-46547	NocoDB is software for building databases as spreadsheets. Prior to 2026.04.1, a reflected XSS vulnerability exists in the Page Leaving Warning page. The ncRedirectUrl and ncBackUrl query parameters are used in window.location.href and <a> tag bindings without validation, allowing javascript: URI injection. This vulnerability is fixed in 2026.04.1.	6.1	More Details
CVE-2026-46770	Vulnerability in the Oracle Application Development Framework (ADF) product of Oracle Fusion Middleware (component: Security Framework). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Application Development Framework (ADF). Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Development Framework (ADF), attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Development Framework (ADF) accessible data as well as unauthorized read access to a subset of Oracle Application Development Framework (ADF) accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2026-46812	Vulnerability in the Oracle Access Manager product of Oracle Fusion Middleware (component: Authentication Engine). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Access Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Access Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Access Manager accessible data as well as unauthorized read access to a subset of Oracle Access Manager accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details
CVE-2026-55423	Langflow is a tool for building and deploying AI-powered agents and workflows. Prior to 1.7.0, the logout button does not clear the session. The previous user stays logged in unless another user explicitly logs in. This vulnerability is fixed in 1.7.0.	6.1	More Details
CVE-2026-50019	yt-dlp is a command-line audio/video downloader. From 2023.09.24 until 2026.06.09, if curl is used as an external downloader for yt-dlp, cookies may be leaked to an unintended host upon HTTP redirect or when the host for download fragments differs from their parent manifest's. At the file download stage, the cookies are passed by yt-dlp to the file downloader via --cookie. However, unless these are loaded from a file, this operation does not activate the cookie engine. As a result, curl will send cookies with requests to domains or paths for which the cookies are not scoped. This vulnerability is fixed in 2026.06.09.	6.1	More Details
CVE-2026-	Langflow is a tool for building and deploying AI-powered agents and workflows. Prior to 1.10.0, the "Shareable Playground" (or "Public Flows" in code) contains a potential arbitrary file-read vulnerability, depending on the exact flow configuration used. By making a flow public, public execution of the flow is allowed. The execution request can contain a list of files that gets read	6.1	More

48520	by Langflow and fed into the LLM. The files path can be any path supported by the storage - it can be either a local file or S3 path if supported by the local configuration This vulnerability is fixed in 1.10.0.		Details
CVE-2026-47833	setupBpmLogs follows symlink for bpm.log open and chown — container-to-host privilege escalation via /etc/shadow. A compromised process inside a bpm container can cause root to chown an arbitrary host file to vcap and append bpm JSON log lines to it. The chown alone lets the attacker take ownership of /etc/shadow and read every password hash on the host via the read-only /etc bind mount. This is a container-to-host confidentiality break affecting every bpm-managed job. Affected versions: bpm-release, all versions prior to v1.4.30.	6.1	More Details
CVE-2026-56263	Crawl4AI before 0.8.7 contains a stored cross-site scripting vulnerability in the monitor dashboard that renders crawl URLs and error messages via innerHTML without escaping. An attacker can submit a crafted crawl request with malicious markup that executes in an operator's browser when viewing the dashboard.	6.1	More Details
CVE-2026-10857	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in AKIN Software Computer Import Export Industry and Trade Ltd. E-Commerce allows Reflected XSS. This issue affects e-Commerce: before 1.25.01.06.	6.1	More Details
CVE-2026-44663	OpenEXR is the reference implementation and specification for the EXR image format, widely used in the motion picture industry. In versions 3.4.0 through 3.4.11, an integer overflow in ht_undo_impl() in src/lib/OpenEXRCore/internal_ht.cpp leads to a heap-buffer overflow when decoding a crafted HTJ2K-compressed EXR file. decode->channels[i].width (int32_t) is multiplied by bytes_per_element in 32-bit signed arithmetic. With large widths (e.g., >= 536870912 for FLOAT data), this overflows, producing a corrupted offset that is later used for pointer arithmetic and can cause a heap out-of-bounds write. The same unchecked multiplication pattern appears in two other HTJ2K paths (bytes-per-line accumulation and pixel-line pointer advancement). As with related CVE-2026-34378 through CVE-2026-34589 fixes in other codecs, validating only after the multiplication is too late because the value may already be overflowed. This issue has been fixed in version 3.4.12.	6.1	More Details
CVE-2026-56697	Nuxt versions 4.0.0 before 4.4.7 and 3.x before 3.21.7 accept protocol-relative paths such as //evil.com in the reloadNuxtApp function; these pass the script-protocol check but resolve to a cross-origin URL against the current page protocol. Attackers can inject paths like //evil.com to redirect users to attacker-controlled hosts, enabling phishing and OAuth authorization-code theft.	6.1	More Details
CVE-2026-56326	Nuxt versions 4.0.0 before 4.4.7 and 3.x before 3.21.7 contain a server-side open redirect vulnerability in navigateTo that fails to properly validate path-normalized payloads like /..//evil.com and /.//evil.com. Attackers can bypass external-host checks using path-normalization techniques to redirect users to attacker-controlled sites via the Location header or meta-refresh, enabling phishing and OAuth authorization-code theft.	6.1	More Details
CVE-2026-44889	WebOb provides objects for HTTP requests and responses. Prior to 1.8.10, the normalization of the HTTP Location header during a redirect is vulnerable to an open redirect: WebOb joins the redirect target to the request URI using Python's urljoin, and since Python 3.10 the underlying urlsplit strips ASCII tab, carriage return, and newline characters before parsing, so a redirect target containing such characters can be reinterpreted as a protocol-relative URL whose authority is an attacker-controlled host. This bypasses the CVE-2024-42353 fix that escaped a leading double slash, allowing an attacker who influences the redirect location to send users to an arbitrary external site instead of the intended one. This vulnerability is fixed in 1.8.10.	6.1	More Details
CVE-2026-44644	LiquidJS is a Shopify/GitHub Pages compatible template engine written in pure JavaScript. Versions 10.25.7 and below are vulnerable to XSS through a flaw in the strip_html filter logic. The strip_html filter is intended to remove HTML tags from a string before rendering, and is widely used as an XSS sanitizer. The implementation uses a regex whose catch-all branch (<.*?>) does not match line terminators, so any HTML tag containing a \n or \r character passes through unmodified. An attacker who can place a newline inside a tag (e.g. <img\nsrc=x\nonerror=alert(1)>) bypasses sanitization entirely, since browsers treat newlines as whitespace within a tag and execute the resulting onerror/onload/etc. handler. Exploitation is possible for applications that both render attacker-controlled strings via {{ x | strip_html }} to defend against HTML injection and do not separately HTML-escape that output (default behavior — outputEscape is unset by default). This issue has been fixed in version 10.26.0.	6.1	More Details

CVE-2026-56698	Nuxt versions 4.0.0 before 4.4.7 and 3.x before 3.21.7 fail to validate script-capable URLs in the navigateTo open option, allowing client-side script execution. Attackers can supply javascript: URLs through the open parameter to execute arbitrary scripts in the application's origin when user-controlled input is passed to navigateTo.	6.1	More Details
CVE-2026-12137	The SysBasics Customize My Account for WooCommerce – Dashboard, Endpoints, Avatar & Menu Manager plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'tab' parameter in all versions up to, and including, 4.3.6 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. Because the vulnerable plugin_options_page() function is only rendered within the WordPress admin dashboard, successful exploitation requires the targeted victim to be logged in with Shop Manager-level access or higher.	6.1	More Details
CVE-2026-54386	marimo before 0.23.9 contains a reflected cross-site scripting vulnerability in the notebook page that allows unauthenticated attackers to inject arbitrary JavaScript by exploiting improper escaping of single quotes in the file query parameter reflected into an inline JavaScript string literal. Attackers can craft a malicious link with a payload beginning with __new__ to bypass the 404 check and inject JavaScript into the page, which executes without Content-Security-Policy restrictions in the origin of a victim's marimo server.	6.1	More Details
CVE-2026-4110	The ultimate-woocommerce-auction-pro WordPress plugin through 2.4.5 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	6.1	More Details
CVE-2026-8059	IBM Datacap 9.1.7, 9.1.8, and 9.1.9 and IBM Datacap Navigator 9.1.7, 9.1.8, and 9.1.9 is vulnerable to cross-site scripting. This vulnerability allows an unauthenticated attacker to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	6.1	More Details
CVE-2025-71331	Flowise before 3.0.8 contains a cross-site scripting (XSS) vulnerability caused by insufficient input filtering in chat messages and custom agent functions. An attacker can inject malicious JavaScript by sending an iframe payload (e.g., <iframe src="javascript:alert(document.cookie)">) in a chat box, or by having a custom agent function return an XSS payload from an external website. The injected script executes in the victim's browser, enabling theft of cookies and session data.	6.1	More Details
CVE-2026-46877	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: VMSVGA device). The supported version that is affected is 7.2.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	6.0	More Details
CVE-2026-46825	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: VMSVGA device). The supported version that is affected is 7.2.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:N/I:H/A:N).	6.0	More Details
CVE-2026-47375	NocoDB is software for building databases as spreadsheets. Prior to 2026.04.1, an authenticated user with columnAdd permission on a Postgres-backed base can inject arbitrary SQL into the formula engine via the optional direction argument of ARRAYSORT(...). The value is unrestricted by formula validation and embedded into a knex.raw ORDER BY clause, executing during column creation and on every subsequent record read of the formula column. The vulnerability is specific to the Postgres mapping for ARRAYSORT in packages/nocodb/src/db/functionMappings/pg.ts. This vulnerability is fixed in 2026.04.1.	6.0	More Details
CVE-	A vulnerability in the vmadmin CLI of Cisco Umbrella Virtual Appliance could allow an authenticated, local attacker to elevate privileges on an affected device. This vulnerability is due		

2026-20246	to insufficient validation of user-supplied commands. An attacker with vmadmin privileges could exploit this vulnerability by using certain commands at the CLI. A successful exploit could allow the attacker to elevate privileges to root.	6.0	More Details
CVE-2026-46768	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: VMSVGA device). The supported version that is affected is 7.2.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 6.0 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H).	6.0	More Details
CVE-2026-44273	Dell Wyse Management Suite (WMS), versions prior to WMS 2605, contain a Use of Default Credentials vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Information Disclosure.	6.0	More Details
CVE-2025-2669	IBM Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data versions 4.8, 5.0, 5.1, 5.2, 5.3 could allow a privileged user to perform operations and obtain sensitive information outside of their authority due to improper token validation.	6.0	More Details
CVE-2026-55748	OpenStack Horizon before 25.7.4 produces scripts for OpenStack RC file downloading that may have a crafted project name with shell metacharacters. NOTE: some parties consider this a security hardening opportunity to address certain types of user error, not a vulnerability.	6.0	More Details
CVE-2026-10852	IBM i 7.6, 7.5, 7.4, and 7.3, IBM WebSphere Application Server, and IBM WebSphere Application Server Liberty are vulnerable to denial of service in the WebSphere WebServer Plug-in component when an attacker can pass crafted requests to the web server.	5.9	More Details
CVE-2026-54323	Daytona is a secure and elastic infrastructure runtime for AI-generated code execution and agent workflows. Prior to 0.185.0, the daemon's git clone implementation disabled TLS certificate verification. When a clone request carried Git credentials, the daemon sent the HTTP Basic Authorization header to the remote over a connection whose certificate was never validated, on both the go-git and native git CLI code paths. An attacker able to intercept clone traffic could present any TLS certificate, capture the Git credentials supplied for the clone, and serve tampered repository content into the sandbox. This vulnerability is fixed in 0.185.0.	5.9	More Details
CVE-2026-9678	Impact: Undici's cache interceptor incorrectly classifies some responses as cacheable when the upstream Cache-Control header uses whitespace-padded qualified private or no-cache field names such as private=" authorization" or no-cache="\tauthorization". The parser preserves the surrounding whitespace, so later comparisons against the literal authorization field name fail and the response is stored. In shared-cache mode, this allows a response containing one user's authenticated data to be served from cache to a subsequent caller, including an unauthenticated caller, when both requests resolve to the same cache key. Affected applications are those that explicitly enable the cache interceptor (interceptors.cache()) in shared mode, forward Authorization headers upstream, and receive cacheable responses with non-canonical qualified private or no-cache directives. Patches: Upgrade to undici v7.28.0 or v8.5.0. Workarounds: If upgrade is not immediately possible, disable shared-cache mode for traffic that includes Authorization headers, avoid caching responses to authenticated requests, or add Vary: Authorization upstream.	5.9	More Details
CVE-2026-56007	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in OceanWP Ocean Product Sharing allows Stored XSS. This issue affects Ocean Product Sharing: from n/a through 2.2.2.	5.9	More Details
CVE-2026-56009	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bricksable for Bricks Builder allows Stored XSS. This issue affects Bricksable for Bricks Builder: from n/a through 1.6.83.	5.9	More Details
CVE-2026-54286	Hono is a Web application framework that provides support for any JavaScript runtime. Prior to 4.12.25, on Windows hosts, an encoded backslash (%5C) in the request path decodes to \, which the Windows path resolver treats as a separator. serve-static then resolves a single URL segment such as admin\secret.txt into a nested file under the root and serves it, letting an attacker read static files meant to be protected behind prefix-mounted middleware. This vulnerability is fixed in 4.12.25.	5.9	More Details

CVE-2026-9679	Impact: undici's cookie parser in parseSetCookie percent-decodes cookie values via qsUnescape, turning encoded sequences like %0D%0A, %00, %3B, and %3D into their literal byte equivalents. RFC 6265 §5.4 does not specify any decoding and browsers do not decode either. Applications that parse a Set-Cookie header and then forward the parsed value into a response header (proxies, middleware, SSR frameworks) become vulnerable to HTTP response header injection: an attacker-controlled upstream can inject arbitrary Set-Cookie, Location, or Cache-Control headers into the application's downstream response, enabling session fixation, open redirect, or cache poisoning. Affected applications are those that use undici's cookie parsing (parseSetCookie, parseCookie, getSetCookies) and forward the parsed cookie value into a response header. This was introduced in undici 7.0.0 via PR #3789. Patches: Upgrade to undici v6.26.0, v7.28.0 or v8.5.0. Workarounds: If upgrade is not immediately possible, do not forward values returned by parseSetCookie/parseCookie/getSetCookies directly into response headers; sanitize the value first to strip or reject CR, LF, NUL, ;, and = bytes.	5.9	More Details
CVE-2026-55199	libssh2 through 1.11.1, fixed in commit 1762685, contains a pre-authentication denial of service vulnerability in the SSH_MSG_EXT_INFO handler in src/packet.c that allows a malicious SSH server to cause a client CPU exhaustion loop by sending a crafted extension count value. A malicious server can set nr_extensions to 0xFFFFFFFF during key exchange, causing the client to spin in a tight CPU loop for over 60 seconds because return values from _libssh2_get_string() are unchecked and the session timeout does not apply to CPU-bound loops.	5.9	More Details
CVE-2026-55568	Guzzle is an extensible PHP HTTP client. Prior to 7.12.1, in certain configurations, traffic expected to be protected by TLS on the hop to the proxy is transmitted in cleartext. Proxy authentication credentials (the Proxy-Authorization header, proxy userinfo in the proxy URL, or CURLOPT_PROXYUSERPWD) are sent without encryption, and the CONNECT target host and port for tunneled HTTPS requests are exposed. The built-in cURL handlers (GuzzleHttp\Handler\CurlHandler and GuzzleHttp\Handler\CurlMultiHandler, used by default whenever the PHP cURL extension is available) accept an https:// proxy. libcurl older than 7.50.2 silently treats an https:// proxy as a plaintext http:// proxy. The TLS connection to the proxy is never established, and the proxy leg is cleartext with no error or warning. An application is affected when it sends requests through one of the built-in cURL handlers, configures an https:// proxy expecting the proxy connection itself to be encrypted, and runs with libcurl older than 7.50.2. This vulnerability is fixed in 7.12.1.	5.9	More Details
CVE-2026-12725	A heap-based buffer overflow was found in dnsmasq. When DNSSEC validation and query logging are both enabled, logging of DS or DNSKEY replies containing unsupported algorithm or digest types can cause dnsmasq to write past the end of an internal logging buffer. A remote attacker able to supply such a DNS response may crash the dnsmasq process, resulting in denial of service.	5.9	More Details
CVE-2026-7850	The WP Magnific Popup WordPress plugin through 1.0 does not properly escape user-controlled link URLs before injecting them into the DOM when displaying image load error messages, allowing authenticated attackers with Author-level access or above to perform Stored Cross-Site Scripting attacks against any visiting user.	5.9	More Details
CVE-2026-9320	IBM WebSphere Application Server 9.0, and 8.5 and IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.6 are vulnerable to a denial of service, caused by sending a specially-crafted request. A remote attacker could exploit this vulnerability to cause the server to consume memory resources.	5.9	More Details
CVE-2026-50202	Steeltoe is an open source project that provides a collection of libraries that helps users build cloud-native applications. In Steeltoe.Security.Authentication.CloudFoundryBase prior to version 3.4.0, Steeltoe.Security.Authentication.JwtBearer prior to version 4.2.0, and Steeltoe.Security.Authentication.OpenIdConnect prior to version 4.2.0, the JWT signing key cache in `TokenKeyResolver` uses `kid` as the sole cache key without namespacing by authority. In applications with multiple `JwtBearer` schemes pointing to different identity providers, a key fetched for one scheme can satisfy token validation for another. Additionally, cached keys have no expiration, so rotated or revoked keys remain trusted until the application process restarts. Steeltoe.Security.Authentication.CloudFoundryBase version 3.4.0, Steeltoe.Security.Authentication.JwtBearer version 4.2.0, and Steeltoe.Security.Authentication.OpenIdConnect version 4.2.0 patch the issue. If an immediate upgrade is not possible: In multi-scheme deployments, configure only one `JwtBearer` scheme per application when different identity providers are required; and/or restart the application process after an identity provider signing key rotation to clear stale cached keys.	5.9	More Details

CVE-2026-55767	Guzzle is an extensible PHP HTTP client. Prior to 7.12.1, CookieJar incorrectly accepts cookies with a dot-only Domain attribute and whitespace-padded variants. SetCookie::matchesDomain() removes leading dots from the cookie domain, normalizing dot-only values to the empty string; SetCookie::validate() only rejected a strictly empty domain, so these cookies could be stored and the empty normalized domain was treated as matching any request host. An attacker-controlled origin that an application requests with a shared cookie jar can therefore set a cookie that Guzzle later sends to unrelated hosts using the same jar. This may allow cookie injection or session fixation against downstream services, depending on how those services interpret the injected cookie. This vulnerability is fixed in 7.12.1.	5.8	More Details
CVE-2026-46552	NocoDB is software for building databases as spreadsheets. Prior to 2026.04.1, shared-base sessions were granted the same base-member capabilities as authenticated viewers. Using only the shared-base UUID (xc-shared-base-id), an attacker could enumerate base members and invite an arbitrary email into the base as a real member. The invited user could then redeem the invite via the normal signup flow and retain authenticated access even after the owner revoked the shared link. Shared-base sessions were mapped to ProjectRoles.VIEWER in packages/nocodb/src/strategies/base-view.strategy/base-view.strategy.ts, and packages/nocodb/src/utils/acl.ts granted baseUserList and userInvite to that role. The shared frontend (packages/nc-gui/composables/useApi/interceptors.ts) deliberately removed auth headers in favour of the shared-base header, but the ACL middleware did not distinguish shared sessions from genuine viewers. This vulnerability is fixed in 2026.04.1.	5.8	More Details
CVE-2026-55599	phpseclib is a PHP secure communications library. From 0.1.1 until 1.0.30, 2.0.55, and 3.0.54, when an application validates an untrusted X.509 certificate with phpseclib, X509::validateSignature() reads a URL out of that certificate's Authority Information Access (AIA) extension and connects to it. Attacker who supplies certificate fully controls host, port, and path of that connection. URL fetching is enabled by default, and no destination is blocked. An unauthenticated attacker can therefore make a validating server open connections to internal hosts and ports it should never reach, for example loopback 127.0.0.1, cloud metadata address 169.254.169.254, and internal-only services. This is a server-side request forgery (SSRF) caused by an insecure default. This vulnerability is fixed in 1.0.30, 2.0.55, and 3.0.54.	5.8	More Details
CVE-2026-44046	Use of Less Trusted Source vulnerability in Apache APISIX. Attacker can take advantage of wolf-rbac plugin under default configuration to potentially pollute logs with spoofed identity information and exploit IP based access control rules. This issue affects Apache APISIX: from 1.2.0 through 3.16.0. Users are recommended to upgrade to version 3.17.0, which fixes the issue.	5.8	More Details
CVE-2026-48983	pam_usb provides hardware authentication for Linux using ordinary removable media. In versions prior to 0.9.2, a symlink race condition exists in per-device and per-user pad directory creation. pam_usb uses a check-then-act pattern: it calls lstat() to test for existence and then calls mkdir() separately to create the directory. A local attacker can win the race between these calls by replacing the target path with a symlink to a directory they control. If successful, one-time pad files may be written to an attacker-controlled location, potentially exposing future pad values before use or disrupting authentication. This issue has been fixed in version 0.9.2.	5.8	More Details
CVE-2026-48982	pam_usb provides hardware authentication for Linux using ordinary removable media. In versions prior to 0.9.2, when updating a one-time pad file, a temporary file is created using open() without the O_EXCL flag. Without O_EXCL, the create operation is not atomic: two concurrent processes racing to update the same pad may both succeed in opening the file, with the second write silently overwriting the first. The one-time pad is the core replay-prevention mechanism of pam_usb. A successful race could result in the stored pad value diverging from what either process expected, potentially causing authentication failures or, in a precisely timed attack, creating a window for pad reuse. This issue has been fixed in version 0.9.2.	5.8	More Details
CVE-2026-48822	Shaarli is a personal bookmarking service. Versions 0.16.1 and prior contain a stored Cross-Site Scripting (XSS) vulnerability in the Markdown-to-HTML conversion process used in the Bookmark Description field. An authenticated user can inject a malicious javascript: URI inside a Markdown link. The vulnerability originates in the filterProtocols method within BookmarkMarkdownFormatter.php.This method attempts to sanitize Markdown links by filtering dangerous protocols (such as javascript:) before rendering. It uses the following regular expression: (#]\((.*?)\)#is). This regex is designed to detect inline Markdown links, but it fails to detect Markdown reference-style links because reference-style links are resolved by the Markdown parser after preprocessing. The filterProtocols method never inspects the actual URL used in these references and as a result, an attacker can supply a javascript: URI inside a	5.8	More Details

	reference definition. This issue has been fixed in version 0.16.2.		
CVE-2026-48821	Shaarli is a personal bookmarking service. Versions 0.16.1 and prior contain a DOM-based Cross-Site Scripting (XSS) vulnerability in the Thumbnail Synchronizer feature. When an administrator runs the thumbnail update process, malicious bookmark titles are returned via an AJAX response and inserted into the DOM using innerHTML without proper sanitization. The issue originates from the interaction between the backend thumbnail update endpoint and the frontend JavaScript responsible for rendering update progress. On the backend, the ThumbnailsController::ajaxUpdate method returns bookmark data formatted using the 'raw' formatter. This includes the unescaped bookmark title in the JSON response. On the client side, the script thumbnails-update.js processes this AJAX response and dynamically updates the progress interface. Administrators using the thumbnail synchronization feature are affected and exploitation could lead to session hijacking, privilege escalation, backdoor injection and full compromise. This issue has been fixed in version 0.16.2.	5.8	More Details
CVE-2026-55706	sppp_pap_input in sys/net/if_spppsubr.c in OpenBSD before 076e2b1 allows authentication bypass via certain zero values for lengths.	5.8	More Details
CVE-2026-35067	Dell PowerFlex Manager, version(s) [Versions], contain(s) an Improper Access Control vulnerability. A low privileged attacker with adjacent network access could potentially exploit this vulnerability, leading to Elevation of privileges and Unauthorized access.	5.7	More Details
CVE-2026-35069	Dell PowerFlex Manager, version(s) [Versions], contain(s) an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability. A low privileged attacker with adjacent network access could potentially exploit this vulnerability, leading to Script injection.	5.7	More Details
CVE-2026-11941	Cloudflare Quiche was affected by 2 use-after-free vulnerabilities in the connection ID iterator FFI functions. The “quiche_connection_id_iter_next” and “quiche_conn_retired_scid_next” functions would return a pointer to a “ConnectionId” to the applications via function arguments, but the owned “ConnectionId” would be dropped at the end of those functions' scope. Only applications using those FFI functions are affected. The FFI API is disabled by default by a build-time feature flag. Impact If unpatched, an application calling the affected FFI functions will dereference freed memory. The most likely outcome is undefined behavior leading to a process crash (denial of service). Depending on allocator state, the read may also return adjacent heap contents, resulting in limited information disclosure or incorrect connection identifier handling. Mitigation Users are requested to upgrade to quiche 0.29.2 which is the earliest version containing the fix for this issue.	5.6	More Details
CVE-2026-2604	A flaw was found in evolution-data-server. Inconsistent comparison logic in the addressbook file backend allows a Flatpak application with D-Bus access to craft a malicious URI containing directory traversal sequences. This URI is stored without proper validation during contact creation or modification. Later, during contact deletion, the URI is processed with a less strict check, leading to the deletion of arbitrary files on the host filesystem. This could potentially include critical Flatpak override files.	5.6	More Details
CVE-2026-28587	In MmsSmsProvider of MmsSmsProvider.java, there is a possible way to retrieve sensitive information due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2026-56074	PraisonAI before 1.5.128 caches tool approval decisions by tool name only, not by invocation arguments, allowing subsequent execute_command calls to bypass approval prompts. Attackers can exploit this by obtaining initial approval for a benign command, then silently exfiltrate API keys and credentials via subsequent shell commands without user consent.	5.5	More Details
CVE-2026-0064	In multiple places, there is a possible persistent denial of service due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2026-28575	In PackageInstaller.Session#transfer of frameworks/base/services/core/java/com/android/server/pm/PackageInstallerSession.java, there is a possible memory exhaustion attack due to a logic error in the code. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-	In Contacts Provider, there is a possible way to access the contacts database due to SQL		More

2026-28576	injection. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	Details
CVE-2026-40722	Missing Authorization vulnerability in Yoast BV Yoast SEO Premium allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Yoast SEO Premium: from n/a through 26.6.	5.5	More Details
CVE-2026-8636	IBM Datacap 9.1.7, 9.1.8, and 9.1.9 and IBM Datacap Navigator 9.1.7, 9.1.8, and 9.1.9 allows an attacker to retrieve user passwords and cryptographic keys from memory. Attacker can use the same keys to decrypt password, gain access to the application and access sensitive data in the database.	5.5	More Details
CVE-2026-39577	Unauthenticated PHP Object Injection in Playroom <= 1.4.1 versions.	5.5	More Details
CVE-2026-39578	Unauthenticated PHP Object Injection in Valiance <= 1.2 versions.	5.5	More Details
CVE-2026-53870	Hermes Agent before 0.16.0 creates response_store.db and webhook_subscriptions.json with world-readable permissions (mode 0o644), exposing conversation history and HMAC secrets to local users. Attackers with local filesystem access can read these files directly to obtain sensitive data including conversation history, tool payloads, prompts, and per-route HMAC secrets.	5.5	More Details
CVE-2026-1288	A maliciously crafted RFA file, when converted to FormIt via “Convert RFA to FormIt” in Autodesk Revit, can force a NULL Pointer Dereference vulnerability. Successful exploitation may cause the application to crash, leading to a denial-of-service condition.	5.5	More Details
CVE-2026-3196	An integer overflow vulnerability was found in the virtio-snd device via PCM_INFO requests from the guest. A malicious guest can provide out-of-bounds stream counts, potentially leading to unbounded memory allocation on the host and a denial of service condition.	5.5	More Details
CVE-2026-48991	XianYuLauncher is a Minecraft Java Edition launcher. In versions prior to 1.5.5, sensitive authentication artifacts could be exposed during a user-initiated login under certain local attack conditions. Affected versions relied on a fixed localhost redirect URI without PKCE or state validation. Exploitation is most likely to occur when an attacker is able to observe, intercept, or otherwise interfere with the local authentication flow on the same device. This issue has been fixed in version 1.5.5.	5.5	More Details
CVE-2026-12444	Out of bounds read in Chromoting in Google Chrome on Windows prior to 149.0.7827.155 allowed a local attacker to obtain potentially sensitive information from process memory via a malicious file. (Chromium security severity: High)	5.5	More Details
CVE-2020-9713	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to disclose sensitive information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-55392	NILFS utilities through 2.3.0, fixed in commit 26efb5d, nilfs_sb_is_valid() function fails to validate s_log_block_size field in NILFS2 superblock before bit-shift operations. Attackers supplying crafted NILFS2 images trigger undefined behavior through oversized shifts or out-of-memory conditions, crashing tools like nilfs-tune and dumpseg.	5.5	More Details
CVE-2020-9711	Acrobat Reader versions 2020.009.20074, 2020.001.30002, 2017.011.30171, 2015.006.30523 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to disclose sensitive information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2026-48985	pam_usb provides hardware authentication for Linux using ordinary removable media. In versions 0.9.1 and below, pusb_is_loginctl_local() can cause a NULL dereference crash when parsing loginctl output. The function calls popen() and reads the result; if the Remote field is only a newline, fgets() succeeds but strtok_r(buf, "\n", &saveptr) returns NULL. A subsequent strcmp(is_remote, "no") then dereferences NULL, causing undefined behavior (typically SIGSEGV) and crashing the PAM module. This can crash the authenticating process (e.g., sudo,	5.5	More Details

	login) and, depending on PAM stack configuration, deny access for all users of the affected service. This issue has been fixed in version 0.9.2.		
CVE-2026-49406	Deno is a JavaScript, TypeScript, and WebAssembly runtime. Prior to 2.7.12, when Deno was run in BYONM mode (nodeModulesDir: "manual"), the module resolver did not validate that a package's resolved entrypoint stayed within its node_modules/<pkg>/ directory. A malicious package.json whose main field contained .. segments was able to resolve to an arbitrary path on disk, and the resolver then read that file without consulting the --allow-read allowlist. This let a require("evil-pkg") call return the contents of a file that a direct Deno.readTextFileSync(...) call would have been blocked from reading. This vulnerability is fixed in 2.7.12.	5.5	More Details
CVE-2026-56692	NanoClaw before 2.1.17 contains a symlink following vulnerability in forwardAttachedFiles that allows container-controlled agents to exfiltrate host-readable files. The host validates attachment filenames using only isSafeAttachmentName before copying with fs.copyFileSync, which follows symlinks without containment checks, allowing malicious agents to disclose arbitrary host files.	5.5	More Details
CVE-2026-56693	NanoClaw before 2.1.17 contains a privilege escalation vulnerability in the create_agent delivery-action handler that performs privileged central-database writes without host-side authorization checks. Confined agent containers can invoke create_agent to create arbitrary agent groups, container configurations, and destinations, escalating beyond their intended confinement boundary.	5.5	More Details
CVE-2026-12163	Fortra File Integrity Monitoring (FIM), formerly Tripwire Enterprise, versions prior to 9.4.0.1 contain a stored cross-site scripting (XSS) vulnerability in the Asset View UI component. An authenticated user with sufficient privileges to create or modify affected node or database configuration fields could store script content that may be rendered as HTML instead of safely escaped text when the affected Asset View UI content is displayed.	5.5	More Details
CVE-2026-28573	In AndroidManifest.xml, there is a possible persistent denial of service due to a missing permission check. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2026-48493	Snipe-IT is an IT asset/license management system. In versions prior to 8.6.0, a user with only users.edit can send a PATCH to /api/v1/users/{their_own_id} and grant themselves any permission except admin and superuser — for example `assets.view`, `assets.create`, `reports.view`, import, etc. The issue is patched in version 8.6.0.	5.5	More Details
CVE-2026-56301	Nuxt 4.0.0 before 4.4.7 and 3.18.0 before 3.21.7, when running the development server (nuxt dev) on Linux, binds the vite-node IPC server to an abstract-namespace Unix socket without permission restrictions, allowing local users to enumerate and connect. Unprivileged co-resident users can exploit the unprotected module request handler to read arbitrary files such as .env and SSH keys through the SSR plugin pipeline. Production builds are unaffected, as the IPC server runs only in development.	5.5	More Details
CVE-2026-11819	Module: plugins/modules/keyring_info.py CVSS 3.1: 5.5 MEDIUM — AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N Issue: The module retrieves a passphrase from the OS native keyring (GNOME Keyring, macOS Keychain, Windows Credential Manager) and places it directly into result["passphrase"] with no output suppression, no no_log protection, and no documentation warning. Root Cause: Line 105 (protected): keyring_password=dict(type="str", required=True, no_log=True) Line 127 (NOT protected): result["passphrase"] = passphrase Observed Output: { "changed": false, "passphrase": "MyMasterP@ssw0rd!SSH_Key_Secret" } Visible via register + debug: { "keyring_result": { "changed": false, "passphrase": "MyMasterP@ssw0rd!SSH_Key_Secret" } } Impact: Master passwords, SSH key passphrases and service credentials appear in all Ansible output register: keyring_result followed by debug: var=keyring_result prints passphrase in full Ansible fact caching backends (Redis, JSON file, memcached) may persist the passphrase AWX/Tower job logs silently store the live credential Fix: module.exit_json(changed=False, passphrase=passphrase, _ansible_no_log=True) Also add a documentation warning requiring callers to use no_log: true at the task level. PoCs Fig 1: PoC execution showing passphrase in plaintext output Fig 2: Source code showing no_log=True on input (line 105) vs unprotected output (line 127)	5.5	More Details
CVE-2026-	Cotonti 1.0.0 (master branch, commit f43f1fc3) is vulnerable to Cross-Site Request Forgery in the Personal File Storage (PFS) module. In modules/pfs/inc/pfs.editfolder.php, the folder update action ('a=update') updates folder metadata (title, description, public/gallery flags) without	5.4	More

55745	calling cot_check_xg() to validate the anti-CSRF token. A remote attacker who lures an authenticated user into visiting a malicious page can force the browser to submit a forged request that modifies the victim's folder metadata, including making a private folder public.		Details
CVE-2025-62198	An authenticated user can perform XSS. This issue affects Apache Atlas versions 2.4.0 and earlier. Users are recommended to upgrade to version 2.5.0, which fixes the issue.	5.4	More Details
CVE-2026-12580	EasyFlow .NET developed by Digiwin has a Stored Cross-Site Scripting vulnerability, allowing authenticated remote attackers to inject persistent JavaScript code executed in users' browsers upon page load.	5.4	More Details
CVE-2025-33128	IBM Engineering Workflow Management 7.0.3 through 7.0.3 Interim Fix 020, and 7.1 through 7.1 Interim Fix 007 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	5.4	More Details
CVE-2026-10601	The Tempo and Loki datasource plugins construct backend HTTP requests by interpolating user-supplied input into URL paths without sanitization, enabling path traversal. A Viewer-role user can: (1) capture admin-configured datasource credentials (secureJsonData custom headers) by traversing to an attacker-controlled endpoint, (2) invoke state-changing admin endpoints on Tempo (e.g. /flush, /shutdown), and (3) exfiltrate internal service data via Loki's CallResource which returns full HTTP response bodies.	5.4	More Details
CVE-2026-46550	NocoDB is software for building databases as spreadsheets. Prior to 2026.04.1, the refresh-token cookie was set with httpOnly: true but missing both the secure flag and the sameSite attribute. Over plain HTTP the cookie could be intercepted on the network; without sameSite, browsers attached it to cross-site POSTs, enabling CSRF against the token-refresh endpoint. This vulnerability is fixed in 2026.04.1.	5.4	More Details
CVE-2026-8378	The Frontend File Manager Plugin WordPress plugin through 23.6 does not sanitise nor escape a filename submitted to the frontend file-rename endpoint before storing it as post meta and rendering it back on the admin File Manager listing, leading to a Stored Cross-Site Scripting vulnerability exploitable by users with Subscriber-level access and above against an administrator viewing the file management interface.	5.4	More Details
CVE-2026-45692	Caddy is an extensible server platform that uses TLS by default. From 2.4.0 until 2.11.3, the authorization layer and the /config traversal layer do not agree on what object the path refers to. In this case, a path authorized for one config object is accepted, but then resolves to a different config object during traversal. This happens because the authorization layer uses string prefix matching and the /config traversal layer parses array indices numerically using strconv.Atoi(). This vulnerability is fixed in 2.11.3.	5.4	More Details
CVE-2026-5139	Mattermost versions 11.7.x <= 11.7.0, 11.6.x <= 11.6.2, 11.5.x <= 11.5.5, 10.11.x <= 10.11.17 fail to enforce administrator authorization on the {{setDefaultInstance}} call within the {{/gitlab connect}} command handler, which allows any authenticated user to overwrite the global default GitLab instance configuration via the {{/gitlab connect <instance-name>}} slash command.. Mattermost Advisory ID: MMSA-2026-00644	5.4	More Details
CVE-2026-43915	Coturn is a free open source implementation of TURN and STUN Server. Versions prior to 4.11.0 contain a stored cross-site scripting (XSS) vulnerability in the web-admin HTTPS interface. An attacker who can create a TURN allocation with a crafted USERNAME value can inject HTML/JavaScript that executes when an authenticated web-admin user views the TURN session list. In configurations using anonymous TURN access (--no-auth), this may be exploitable without TURN credentials. In authenticated deployments, exploitation requires valid TURN credentials or control over a provisioned username. This issue has been fixed in version 4.11.0.	5.4	More Details
CVE-2026-11372	IBM TRIRIGA Application Platform 5.0.2 through 5.0.3 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	5.4	More Details
CVE-2026-56696	OpenHarness /issue and /pr_comments slash commands lack remote_invocable=False protection, allowing remote channel senders to write attacker-controlled Markdown into project context files. Admitted remote attackers can inject malicious content into .openharness/issue.md and .openharness/pr_comments.md files, which are subsequently	5.4	More Details

	injected into runtime system prompts, persistently influencing local agent behavior.		
CVE-2026-56694	NanoClaw before 2.1.0 contains a privilege escalation vulnerability in the channel-registration approval flow where handleChannelApprovalResponse fails to validate admin privileges over target agent groups. Scoped admins can submit forged or stale connect callback values to wire messaging channels into out-of-scope agent groups, exposing unauthorized groups to unapproved channels and enabling unauthorized observation or control of restricted agent group activity.	5.4	More Details
CVE-2026-49231	Authentication Bypass by Spoofing vulnerability in opa plugin. An attacker could relay spoofed identity headers to upstream capitalising on non-default configuration in opa plugin. This could allow the attacker to assume higher privileges on the upstream service. This issue affects Apache APISIX: from 3.5.0 through 3.16.0. Users are recommended to upgrade to version 3.17.0, which fixes the issue.	5.4	More Details
CVE-2026-41479	Authlib is a Python library which builds OAuth and OpenID Connect servers. Prior to 1.6.10 and 1.7.1, Authlib's OAuth 2.0 authorization endpoint can be turned into an unauthenticated open redirect when a request uses an unsupported response_type and supplies an attacker-controlled redirect_uri. The vulnerable behavior happens before client lookup and before any redirect URI validation. As a result, an attacker does not need a valid client registration, an authenticated user, or any prior state. A single request to the authorization endpoint is enough to obtain a 302 Location response to an arbitrary attacker-controlled URL. This vulnerability is fixed in 1.6.10 and 1.7.1.	5.4	More Details
CVE-2026-44311	Fabric.js is a Javascript HTML5 canvas library. Prior to 7.4.0, a potential Cross-Site Scripting (XSS) vulnerability exists in Fabric.js due to improper escaping of user-controlled input during SVG serialization via the toSVG() method. Specifically, the color field within the colorStops array of a fabric.Gradient object is not properly escaped when converted into SVG <stop> elements. If an application renders the generated SVG string into the DOM, this may allow an attacker to inject arbitrary HTML/SVG and execute JavaScript in the victim's browser. This vulnerability is fixed in 7.4.0.	5.4	More Details
CVE-2026-10850	Plane CE 1.3.1 allows a low-privileged project member to submit arbitrary HTML/JS in the description_html field when creating an intake work item through the API v1 intake endpoint.	5.4	More Details
CVE-2026-12528	A flaw was found in 389 Directory Server in the __aclp__normalize_acltxt() function of aclparse.c. A malformed ACI (Access Control Instruction) string can trigger heap-buffer-overflow writes and reads during ACI parsing. The function fails to validate that the ACI keyword has sufficient length after whitespace stripping, leading to a 1-byte out-of-bounds write and subsequent out-of-bounds reads. An authenticated user with write access to the aci attribute could send a crafted ACI value to silently corrupt heap memory in the directory server process.	5.4	More Details
CVE-2026-56227	Capgo before 12.128.2 contains a server-side request forgery vulnerability in webhook URL validation that allows loopback and internal addresses. Organization admins can configure webhooks pointing to localhost or 127.0.0.1, and when triggered, the backend performs outbound requests to these addresses with error responses disclosed to users.	5.4	More Details
CVE-2026-12770	A vulnerability was determined in BerriAI litellm up to 1.63.1. The impacted element is an unknown function of the file litellm/proxy/management_endpoints/key_management_endpoints.py of the component Admin Key Handler. This manipulation causes improper authorization. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized. Patch name: 23781. It is recommended to apply a patch to fix this issue. The vendor was contacted early about this disclosure.	5.4	More Details
CVE-2026-55205	Hermes WebUI before 0.51.468 contains a resource exhaustion vulnerability in the unauthenticated POST /api/onboarding/oauth/start endpoint that allows unbounded accumulation of in-memory flow state and daemon threads. Attackers can send repeated or concurrent requests to exhaust server memory and thread resources, potentially triggering repeated outbound device-code requests to upstream OAuth providers.	5.3	More Details
CVE-2026-	Capgo (backend Supabase edge functions) before 12.128.2 does not apply the global authentication middleware to the GET /private/role_bindings/:org_id endpoint, unlike the POST and DELETE role_bindings routes, so unauthenticated requests reach the handler instead of being rejected at the middleware layer. The handler still performs its own authorization check	5.3	More

56321	and returns Unauthorized, so no direct data exposure occurs; the flaw is inconsistent authentication enforcement across HTTP methods that could enable authorization bypass if the handler logic changes.		Details
CVE-2026-8383	The LearnPress WordPress plugin before 4.3.7 does not gate the `edit` context on one of its REST endpoint behind the `edit_users` capability, allowing unauthenticated visitors to retrieve each returned user's roles, full capabilities map, extra capabilities, locale, and registration date via a crafted request	5.3	More Details
CVE-2026-44646	LiquidJS is a Shopify/GitHub Pages compatible template engine written in pure JavaScript. In versions 10.25.7 and below, Context.spawn() creates a child Context for the {% render %} tag but does not propagate the parent context's resolved ownPropertyOnly value, resulting in a silent bypass. The new context re-derives ownPropertyOnly from opts.ownPropertyOnly (the instance-level option), silently discarding any RenderOptions.ownPropertyOnly override that was supplied to parseAndRender(). As a result, a developer who runs a Liquid instance with the backwards-compatible ownPropertyOnly:false and then locks down an untrusted render with parseAndRender(..., { ownPropertyOnly: true }) still leaks prototype-chain properties from inside any {% render %} partial. This is a distinct exploit surface from the previously identified array-filter variants (where, reject, group_by, find, find_index, has) — the underlying root cause in Context.spawn() is shared, but {% render %} is a separately reachable sink that needs no filter usage. This issue has been fixed in version 10.26.0.	5.3	More Details
CVE-2026-54236	vLLM is an inference and serving engine for large language models (LLMs). Prior to 0.23.1rc0, the fix for CVE-2026-22778, which introduced a sanitize_message helper that strips object-repr memory addresses from error messages before they reach the client, is incomplete: several response paths echo str(exc) directly to clients without calling sanitize_message. The unsanitized sites include the Anthropic API router in vllm/entrypoints/anthropic/api_router.py (the POST /v1/messages and POST /v1/messages/count_tokens handlers), the Server-Sent Events streaming converter in vllm/entrypoints/anthropic/serving.py, and the realtime speech-to-text WebSocket in vllm/entrypoints/speech_to_text/realtime/connection.py. These paths catch the exception inside the route coroutine and construct the JSONResponse themselves, bypassing the sanitizing global FastAPI exception handler, and WebSocket frames do not traverse that handler chain at all. Using the same primitive as the parent issue, an unauthenticated attacker can send malformed image bytes through the Anthropic Messages API image content parts so that PIL.Image.open raises an UnidentifiedImageError whose message contains the BytesIO object repr, leaking the heap memory address verbatim in the error.message field of the response body. This vulnerability is fixed in 0.23.1rc0.	5.3	More Details
CVE-2026-56099	OpenBSD before commit 6a23123 (2026-06-18) contains an out-of-bounds read vulnerability in the mpls_do_error function within sys/netmpls/mpls_input.c that allows remote attackers to disclose kernel stack memory by sending crafted MPLS frames with 16 labels and no Bottom-of-Stack bit set.	5.3	More Details
CVE-2026-56213	Capgo before 12.128.2 contains an authorization bypass vulnerability in the public.upsert_version_meta SECURITY DEFINER function exposed via PostgREST RPC, allowing unauthenticated attackers to insert arbitrary rows into version_meta for any app_id. Attackers can exploit this by calling the RPC endpoint with a public anon key to poison storage metrics, causing persistent false data in dashboards and triggering incorrect alerts across victim applications.	5.3	More Details
CVE-2026-56234	Capgo before 12.128.2 contains a credential validation vulnerability in the POST /functions/v1/private/validate_password_compliance endpoint that is callable using only the public Supabase key without authentication. The endpoint is CORS-permissive with wildcard origin allowance and lacks rate limiting, enabling attackers to perform password spraying and credential stuffing attacks to compromise user accounts.	5.3	More Details
CVE-2026-54665	Apache NiFi 0.0.1 through 2.9.0 support building qualified URLs from one of several HTTP request headers that provide an alternative to the standard Host header without validating the values provided. Apache NiFi 1.6.0 introduced a configurable application property to restrict values provided in the HTTP Host header, but did not apply the validation to alternative Proxy and Forwarded headers. The absence of proxy host header validation allowed a client to instruct Apache NiFi web services to construct invalid qualified URLs for redirection or data references. Upgrading to Apache NiFi 2.10.0 is the recommended mitigation, which implements validation for the X-ProxyHost and X-Forwarded-Host HTTP request headers based on the	5.3	More Details

	nifi.web.proxy.host property. Enabling header validation requires configuring the application with HTTPS. Reverse proxy servers in front of Apache NiFi are responsible for filtering input request headers and providing allowed values to the application.		
CVE-2026-47847	Bitnami MariaDB Galera container images and Helm chart are affected by a hardcoded default credential vulnerability in the Galera replication health-check user. The MARIADB_REPLICATION_USER and MARIADB_REPLICATION_PASSWORD environment variables defaulted to monitor and monitor respectively. This user is granted REPLICATION CLIENT privileges from any host ('%'). The Bitnami Helm chart for MariaDB Galera did not expose parameters to configure this user's credentials, resulting in all chart deployments using this publicly known credential by default. Affected versions — Container image: 10.6.x prior to 10.6.27-photon-5-r0; 10.11.x prior to 10.11.17-photon-5-r1; 11.4.x prior to 11.4.12-photon-5-r0; 11.8.x prior to 11.8.7-photon-5-r1; 12.3.x prior to 12.3.2-photon-5-r0 / 12.3.2-debian-12-r0. Helm chart: prior to 18.3.0.	5.3	More Details
CVE-2026-56762	Hono before 4.12.12 does not validate cookie names on the write path in the setCookie(), serialize(), and serializeSigned() functions, allowing invalid characters such as control characters (e.g. \r or \n) when an application passes a user-controlled cookie name. This can produce malformed Set-Cookie header values. In modern runtimes such as Node.js and Cloudflare Workers, such invalid header values are rejected and cause a runtime error before the response is sent, so header injection or response splitting could not be reproduced; the issue primarily affects correctness and robustness, resulting in runtime errors (availability) rather than confirmed header injection.	5.3	More Details
CVE-2026-12969	An out-of-bounds read vulnerability exists in dnsmasq's find_soa() function in src/rfc1035.c. When parsing NS section records, extract_name() is called with extrabytes=0, failing to validate that 10 additional bytes exist for fixed-length DNS record fields. A remote attacker controlling a DNS zone can exploit this via a crafted NXDOMAIN response to cause a 10-byte heap out-of-bounds read, potentially accessing stale data from prior transactions.	5.3	More Details
CVE-2024-33909	Missing Authorization vulnerability in Avirtum iPages Flipbook allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects iPages Flipbook: from n/a through 1.5.1.	5.3	More Details
CVE-2026-9692	Mojolicious::Sessions::Storable versions through 0.05 for Perl generate session ids insecurely. The default session id generator returns a SHA-1 hash seeded with the built-in rand function, the epoch time, the heap address of an anonymous hash, and the PID. These are predictable or low-entropy sources that are unsuitable for security purposes.	5.3	More Details
CVE-2026-48990	joserfc is a Python library that provides an implementation of several JSON Object Signing and Encryption (JOSE) standards. In versions 1.3.4 through 1.6.5, joserfc accepts oversized RFC7797 b64=false JWS payloads without applying JWSRegistry.max_payload_length, which can lead to resource exhaustion. The normal JWS compact and flattened JSON paths reject payloads above the configured payload-size limit with ExceededSizeError. The RFC7797 unencoded payload paths do not make the same check. A valid b64=false compact or flattened JSON JWS can therefore deserialize successfully with a payload larger than JWSRegistry.max_payload_length. Applications that accept lower-trust JWS values and rely on joserfc to reject oversized token content during verification have a moderate availability risk. This issue has been fixed in version 1.6.7.	5.3	More Details
CVE-2026-10530	The Pie Register WordPress plugin before 3.8.4.10 does not use sufficiently random values when generating its account verification tokens, allowing unauthenticated attackers to predict a valid token and activate an account without access to the associated email inbox.	5.3	More Details
CVE-2026-56022	Webmin accepts basic authentication without session cookies when an attacker provides the 'User-Agent: webmin' header, allowing bypass of additional MFA requirements. Fixed in 2.641.	5.3	More Details
CVE-2026-56021	Webmin allows unauthenticated attackers to read the contents of any file ending in .conf within module directories, due to a bypassable regex pattern.	5.3	More Details
CVE-2026-56311	Capgo before 12.128.2 contains an authorization bypass vulnerability in the public.get_current_plan_max_org RPC function that allows unauthenticated attackers to retrieve arbitrary organization plan limits. Attackers can call the RPC endpoint with any organization UUID using only the public Supabase key to disclose billing information including MAU,	5.3	More Details

	bandwidth, storage, and build time limits for any organization.		
CVE-2026-10034	The WP DSGVO Tools (GDPR) plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 3.1.39. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to supply an arbitrary victim email address and trigger immediate SAR processing via the process_now and is_ajax parameters, receiving tokenized download links (zip_link, pdf_link) in the HTTP response that expose the victim's personal data — including WordPress account details, comment author names, email addresses, IP addresses, and comment content — without any proof of ownership. The nonce used for the CSRF check is publicly rendered by the SAR shortcode form and is shared across all anonymous visitors, meaning any unauthenticated attacker can trivially obtain a valid nonce and bypass this gate entirely.	5.3	More Details
CVE-2026-12644	Versions of the package ts-deepmerge before 8.0.0 are vulnerable to Uncaught Exception due to the improper handling of built-in Object.prototype methods (such as toString, valueOf). When user-controlled input contains these keys with non-function values, the resulting merged object becomes broken — any string context operation throws a TypeError, crashing the application.	5.3	More Details
CVE-2026-48988	markdown-it is a Markdown parser. Versions 14.1.1 and below contain a denial-of-service vulnerability when typographer: true is enabled, due to quadratic (O(n^2)) processing in the smartquotes rule. The issue stems from repeatedly modifying strings with replaceAt(), which performs O(n) slicing and concatenation per quote character. This can cause excessive CPU consumption when parsing quote-heavy, user-supplied markdown and may let attackers degrade or disrupt service availability. Although typographer is disabled by default, many production apps enable it for smart typography, making the issue relevant. This issue has been fixed in version 14.2.0.	5.3	More Details
CVE-2026-53550	js-yaml is a JavaScript YAML parser and dumper. Prior to 4.2.0, a crafted YAML document can trigger algorithmic CPU exhaustion in js-yaml merge-key processing (<<) by repeating the same alias many times in a merge sequence. This causes quadratic parse-time behavior relative to input size and can block a Node.js worker/event loop for seconds with a relatively small payload (tens of KB), resulting in denial of service. The issue is in merge handling inside lib/loader.js. This vulnerability is fixed in 4.2.0.	5.3	More Details
CVE-2026-7253	IBM Watson Speech Services Cartridge is vulnerable to Server-Side Request Forgery (SSRF) in Sterling File Gateway, due to a flaw which may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks [GHSA-rr7j-v2q5-chgv] [CVE-2026-7253]. IBM Sterling File Gateway is used in our speech runtimes. This vulnerabilitiy has been addressed. Please read the details for remediation below.	5.3	More Details
CVE-2026-54269	protobufjs compiles protobuf definitions into JavaScript (JS) functions. Prior to 8.6.0 and 7.6.3, protobufjs accepted certain schema-derived names that could collide with properties used by protobufjs runtime helpers. The known affected names are fields named hasOwnProperty, field or oneof names such as $type when loaded through protobufjs JSON/reflection descriptors, and service methods whose generated helper name is rpcCall. When affected message or service types were used, protobufjs could read schema-controlled data where it expected an own-property helper, reflected type metadata, or the base RPC helper. This could cause deterministic exceptions or recursive calls in affected decode post-checks, verification, object conversion, reflected JSON serialization, or protobufjs RPC helper invocation. This vulnerability is fixed in 8.6.0 and 7.6.3.	5.3	More Details
CVE-2026-54270	protobufjs compiles protobuf definitions into JavaScript (JS) functions. From 8.2.0 to 8.4.2, protobufjs preserved unknown wire elements in message.$unknowns and did not provide a decode-time option to discard unknown fields before retaining them. A crafted protobuf payload containing many unknown fields could therefore cause a decoded message to retain substantially more memory than the input size would suggest, even when unknown-field round-tripping is not needed. protobufjs 8.5.0 added the relevant decode-time options, allowing applications that decode untrusted protobuf data to disable unknown-field retention during decode. protobufjs 8.6.2 flips the default so unknown fields are discarded unless explicitly opted into.	5.3	More Details
CVE-	opentelemetry-js is the OpenTelemetry JavaScript Client. Prior to 2.8.0, W3CBaggagePropagator.extract() in @opentelemetry/core does not enforce size limits when parsing inbound baggage HTTP headers. The W3C Baggage specification recommends a		More

2026-54285	maximum of 8,192 bytes and 180 entries; these limits were only enforced on the outbound (inject()) path, not on the inbound (extract()) path. Parsing oversized baggage causes memory allocation proportional to the header size without any cap. This vulnerability is fixed in 2.8.0.	5.3	Details
CVE-2023-33854	IBM Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data versions 4.8, 5.0, 5.1, 5.2, and 5.3 could allow an authenticated user to bypass client-side validation and manipulate input data using man in the middle techniques.	5.3	More Details
CVE-2026-48141	There is a memory leak in NI grpc-device BeginSidebandStream that may result in denial of service due to memory exhaustion. This affects NI grpc-device 2.17.0 and prior versions.	5.3	More Details
CVE-2026-54287	Hono is a Web application framework that provides support for any JavaScript runtime. Prior to 4.12.25, on AWS Lambda, the ALB single-header response and the VPC Lattice v2 response join multiple Set-Cookie headers into one comma-separated value. Because commas also appear inside cookie attributes (for example Expires dates), clients cannot split the value back into individual cookies and silently drop or misparse them. This vulnerability is fixed in 4.12.25.	5.3	More Details
CVE-2026-48166	Filament is a collection of full-stack components for accelerated Laravel development. From 4.0.0 until 4.11.5 and 5.6.5, the login page has an observable timing discrepancy that allows unauthenticated attackers to enumerate registered email addresses. The impact is limited to disclosing whether an account exists for a given email. This vulnerability is fixed in 4.11.5 and 5.6.5.	5.3	More Details
CVE-2026-8049	In SignalRGB versions prior to 1.3.7.0, the \\.\SignalIo device object is created without an explicit SDDL security descriptor and without FILE_DEVICE_SECURE_OPEN. This results in overly permissive default access control, allowing any authenticated local user to obtain a handle to the device and issue privileged IOCTLs.	5.3	More Details
CVE-2026-12565	The unarchive internal module's archive extraction commands perform no code-level validation on extracted file paths, relying entirely on the behavior of external tools (e.g. GNU tar) which varies by platform. While CVE-2025-10284 addressed git-specific RCE vectors, the underlying archive extraction path traversal was never fixed. On systems with GNU tar < 1.34 (Ubuntu 20.04, Debian Buster, CentOS 7, many Docker base images), a malicious archive can write files outside the intended extraction directory.	5.3	More Details
CVE-2026-49342	YARD is a documentation generation tool for the Ruby programming language. Prior to version 0.9.44, YARD's static cache lookup reads a request path before the router's path cleanup runs. When a server is configured with a document root, a traversal path such as `/../yard-cache-secret.html` is joined against that root and can return a readable sibling `.html` file outside the intended static tree. Version 0.9.44 patches the issue.	5.3	More Details
CVE-2026-54300	@astrojs/netlify is an adapter that allows Astro to deploy your hybrid or server rendered site to Netlify. Prior to 7.0.13, @astrojs/netlify converts Astro image.remotePatterns into Netlify Image CDN images.remote_images regular expressions with broader semantics than Astro's canonical matcher. A single wildcard hostname such as *.example.com is converted to an optional subdomain regex, so the apex host matches. A single wildcard pathname such as /ok/* is converted without end anchoring, so deeper paths match by prefix. This vulnerability is fixed in 7.0.13.	5.3	More Details
CVE-2026-6798	The 2Download Connector for 2DL Hosted Checkout plugin for WordPress is vulnerable to unauthorized access in all versions up to, and including, 0.1.5. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to view arbitrary customers' subscription data including subscription status, product names, order IDs, purchase dates, and expiry dates.	5.3	More Details
CVE-2026-48817	Starlette is a lightweight ASGI framework/toolkit. In versions 1.0.1 and below, when dispatching a request, HTTPEndpoint selects the handler by lowercasing the HTTP method and looking it up as an attribute with getattr, without restricting the lookup to a known set of HTTP verbs. When an HTTPEndpoint subclass is registered through Route(...) without an explicit methods= argument, the route does not constrain the method and every method reaches the endpoint. If a non-standard HTTP method whose lowercased name matches an attribute on the endpoint subclass reaches the endpoint, that attribute is invoked as if it were a request handler. An attacker can use this to reach methods that were never meant to be HTTP handlers, such as internal helpers, without the authorization checks applied by the intended public handler. An	5.3	More Details

	application (including Starlette-based frameworks like FastAPI) is affected if it registers an HTTPEndpoint subclass via Route(...) without explicitly setting methods=, and that subclass includes extra methods named like non-standard HTTP verbs that take one request argument and return a response. This issue has been fixed in version 1.1.0.		
CVE-2026-3640	The STRABL – A checkout solution plugin for WordPress is vulnerable to Missing Authentication in all versions up to and including 4.5. The plugin registers a REST API webhook endpoint at /wp-json/strabl/webhook/order with a permission_callback of __return_true, which allows all incoming requests without any authentication or authorization checks. No shared secret, signature validation, HMAC verification, or token-based authentication is implemented. This makes it possible for unauthenticated attackers to create fraudulent WooCommerce orders and mark them as completed by supplying paymentStatus=paid, manipulate existing order statuses by providing an externalOrderId, create new WordPress user accounts with the customer role, issue refunds on existing orders, cancel existing orders, and apply chargeback fees — all without making a legitimate payment or having any valid credentials.	5.3	More Details
CVE-2026-10029	The Event Koi Lite – Events Calendar, Event Management, RSVP, and Tickets plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.3.13.1 via the get_events. This makes it possible for unauthenticated attackers to extract sensitive data including virtual meeting URLs, physical location data, latitude/longitude coordinates, Google Maps links, and RSVP configuration belonging to draft, pending, and private events that are otherwise inaccessible via public URLs.	5.3	More Details
CVE-2026-7859	The Motors WordPress plugin before 1.4.110 does not have proper authorisation and CSRF checks on one of its AJAX actions, allowing unauthenticated attackers to modify arbitrary post metadata, such as the gallery, featured image and, on WooCommerce sites, product prices.	5.3	More Details
CVE-2026-46790	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	5.3	More Details
CVE-2026-56115	dhcpcd through 10.3.2, fixed in commit 2f00c7b, contains a one-byte stack out-of-bounds write vulnerability in dhcp6_makemessage() in src/dhcp6.c that allows unauthenticated same-link attackers to write beyond a fixed local buffer by serializing an oversized RFC6603 OPTION_PD_EXCLUDE option body. Attackers can send a crafted DHCPv6 ADVERTISE message containing an IA_PD IAPREFIX /0 with a valid OPTION_PD_EXCLUDE using an exclude prefix length of /121 through /128 to trigger the out-of-bounds write and potentially corrupt adjacent stack memory.	5.3	More Details
CVE-2026-42489	[This CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] To create and manage guests, domctl operations are used by the control domain, a possible Xenstore domain, or by a domain controlling a particular guest. Some of these operations may not be executed in parallel, so a system-wide lock is used. The way that lock is acquired is, however, not providing any fairness. This is CVE-2026-42489. Furthermore, with XSM/Flask in use, the lock acquire will, for some operations, occur ahead of any permission checking. This is CVE-2026-42490.	5.3	More Details
CVE-2026-54022	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.8.11, the ydoc:document:join Socket.IO handler checks note ownership only when the document_id starts with note: (colon). However, the YdocManager storage layer normalizes all document IDs by replacing colons with underscores (document_id.replace(":", "_")). An attacker can join a document room using note_<id> (underscore) instead of note:<id> (colon), bypassing the authorization check entirely while accessing the same underlying Yjs document. The server then returns the full document state, leaking the victim's private note contents. This vulnerability is fixed in 0.8.11.	5.3	More Details
CVE-2026-12120	The FireBox Popups – Increase Sales and Grow Your Email List plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.1.7 via the 'form_id' parameter. This makes it possible for unauthenticated attackers to extract download a full CSV export of all form submissions — including any personally identifiable information submitted by users — for any arbitrary form_id.	5.3	More Details
	The Simple Membership plugin for WordPress is vulnerable to authorization bypass in all		

CVE-2026-12093	versions up to, and including, 4.7.5. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to deactivate arbitrary member accounts by forging a charge.refunded webhook event containing a victim's subscription ID, setting the target member's account_state to 'inactive' and triggering cancellation hooks, transaction-record status changes, and cancellation notification emails. This vulnerability is exploitable only on installations where no Stripe webhook signing secret has been configured, which is the default out-of-the-box state; sites that have configured the stripe-webhook-signing-secret option are routed to the properly verified HMAC path and are not affected.	5.3	More Details
CVE-2026-56218	Capgo before 12.128.2 fails to strip EXIF metadata including GPS geolocation data from uploaded images, allowing information disclosure. Attackers can download uploaded images and extract precise latitude and longitude coordinates revealing user physical location at capture time.	5.3	More Details
CVE-2026-56282	Capgo before 12.128.2 contains an information disclosure vulnerability in the unauthenticated /replication endpoint that exposes internal PostgreSQL replication telemetry including slot names and WAL LSN positions. Attackers can access this endpoint without authentication to retrieve sensitive infrastructure details such as replication slot names, confirmed_flush_lsn, restart_lsn values, and database error messages for reconnaissance purposes.	5.3	More Details
CVE-2026-12238	The WP Go Maps – Most Popular Map Plugin plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 10.1.01. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to create arbitrary records in plugin database tables (maps, markers, circles, polygons, polylines, rectangles, and point labels) by supplying a WPGMZA-namespaced CRUD-backed class name via the phpClass parameter. The namespace validation check (requiring the 'WPGMZA' prefix) does not prevent exploitation because classes such as WPGMZA\Map and WPGMZA\Marker satisfy it while still triggering an INSERT into the corresponding plugin table before the route rejects the request.	5.3	More Details
CVE-2026-54514	jackson-databind contains the general-purpose data-binding functionality and tree-model for Jackson Data Processor. From 2.0.0 until 2.18.8, 2.21.4, and 3.1.4, JDKFromStringDeserializer constructed InetSocketAddress with new InetSocketAddress(host, port), which performs eager DNS name resolution for hostname inputs at deserialization time. An application that binds untrusted JSON into a type containing an InetSocketAddress field issues an attacker-chosen DNS query during readValue, before any application-level validation or connect logic. The fix uses InetSocketAddress.createUnresolved(host, port), deferring DNS to an explicit connect. This vulnerability is fixed in 2.18.8, 2.21.4, and 3.1.4.	5.3	More Details
CVE-2026-54515	jackson-databind contains the general-purpose data-binding functionality and tree-model for Jackson Data Processor. From 2.8.0 until 2.18.9, 2.21.5, and 3.1.4, in BeanDeserializerBase.createContextual(), per-property @JsonIgnoreProperties exclusions are applied by _handleByNameInclusion(), producing a contextual deserializer whose BeanPropertyMap has the ignored properties removed. The subsequent per-property case-insensitivity block (triggered by @JsonFormat(ACCEPT_CASE_INSENSITIVE_PROPERTIES)) rebuilds from this._beanProperties (the original, unfiltered map) instead of contextual._beanProperties, then overwrites the filtered map — restoring every property _handleByNameInclusion had just removed. The ignored property becomes writable again. This vulnerability is fixed in 2.18.9, 2.21.5, and 3.1.4.	5.3	More Details
CVE-2026-12822	A vulnerability was identified in langflow-ai langflow up to 1.9.3. This affects an unknown function of the component Bundle URL Loader. The manipulation leads to code injection. The attack needs to be performed locally. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2026-54516	jackson-databind contains the general-purpose data-binding functionality and tree-model for Jackson Data Processor. From 2.21.0 until 2.21.4 and 3.1.4, POJOPropertiesCollector._renameProperties() allows a property with @JsonProperty("renamed") on the getter and @JsonIgnore on the setter to be renamed rather than dropped. With MapperFeature.INFER_PROPERTY_MUTATORS enabled (default), the private backing field is retained; during deserialization BeanDeserializerFactory.addBeanProps() sees hasField()==true, builds a FieldProperty, and makes the backing field writable. An attacker supplying the renamed JSON key writes the backing field directly, bypassing the @JsonIgnore on the setter. This vulnerability is fixed in 3.1.4.	5.3	More Details

CVE-2026-56114	dhcpcd through 10.3.2, fixed in commit 2f00c7b, contains a one-byte stack out-of-bounds write vulnerability in dhcp6_makemessage() in src/dhcp6.c that allows unauthenticated same-link attackers to write beyond a fixed local buffer by serializing an oversized RFC6603 OPTION_PD_EXCLUDE option body. Attackers can send a crafted DHCPv6 ADVERTISE message containing an IA_PD IAPREFIX /0 with a valid OPTION_PD_EXCLUDE using an exclude prefix length of /121 through /128 to trigger the out-of-bounds write and potentially corrupt adjacent stack memory.	5.3	More Details
CVE-2025-15657	Unauthenticated Insecure Direct Object References (IDOR) in School Management <= 93.1.0 versions.	5.3	More Details
CVE-2026-54105	The U.S. Government Accountability Office (GAO) Electronic Protest Docketing System (EPDS) and Civilian Board of Contract Appeals (CBCA) Electronic Docketing System (EDS) expose sensitive account information through the 'update-profile/' API endpoint. A remote, unauthenticated attacker can submit a request containing an arbitrary 'user_id' parameter and receive a JSON response containing account-specific information, including the associated email address.	5.3	More Details
CVE-2026-56299	Capgo before 12.128.2 contains an authentication bypass vulnerability in the /build/upload/:jobId/* endpoint that allows unauthenticated attackers to trigger consistent 500 errors. Remote attackers can send OPTIONS requests to bypass authentication middleware and invoke tusProxy logic with invalid credentials, enabling trivial request flooding and denial of service.	5.3	More Details
CVE-2026-56113	dhcpcd through 10.3.2, fixed in commit 5733d3c, contains a heap use-after-free vulnerability that allows unauthenticated same-link attackers to crash the daemon by sending a crafted DHCPv6 RENEW reply with RFC6603 OPTION_PD_EXCLUDE and both preferred and valid lifetimes set to zero. Attackers acting as or impersonating a DHCPv6 server can trigger dhcp6_deprecatedele() to free a delegated child address while an outer TAILQ_FOREACH_SAFE iterator in dhcp6_deprecateaddrs() still holds the freed pointer, causing a use-after-free when TAILQ_REMOVE is reached.	5.3	More Details
CVE-2026-56316	Cap-go before 12.128.2 contains an information disclosure vulnerability in the OPTIONS /build/upload/:jobId/* endpoint that allows unauthenticated attackers to enumerate valid builder job IDs through observable response discrepancies. Attackers can probe the endpoint without authentication to distinguish valid job IDs from invalid ones and generate sustained unauthenticated traffic for resource consumption.	5.3	More Details
CVE-2026-56235	Cap-go capgo before 12.128.2 contains an authorization bypass in several Supabase PostgREST RPC functions (get_app_metrics, get_global_metrics, get_total_metrics) that are granted to the anon role without enforcing org membership or permission checks. An unauthenticated attacker using only the public Supabase API key (sb_publishable_*) can query arbitrary org_id values to disclose cross-tenant usage telemetry (MAU, bandwidth, installs, gets), enumerate app IDs for a target org, and determine org existence via an oracle (valid org returns metrics, invalid returns []).	5.3	More Details
CVE-2026-54517	jackson-databind contains the general-purpose data-binding functionality and tree-model for Jackson Data Processor. From 2.21.0 until 2.21.4 and 3.1.4, in BeanDeserializer._deserializeUsingPropertyBased, the active-view (@JsonView) filter was applied only to creator properties; the regular property-buffering branch performed no prop.visibleInView(activeView) check. A change making SetterlessProperty.isMerging() return true routed setterless Collection/Map properties through this unguarded path, so a setterless collection annotated with a restricted @JsonView is populated from attacker JSON even when the active view excludes it. This vulnerability is fixed in 2.21.4 and 3.1.4.	5.3	More Details
CVE-2026-49983	Deno is a JavaScript, TypeScript, and WebAssembly runtime. Prior to 2.8.1, environment access is gated by the env permission. You can deny it with --deny-env, or restrict it to a specific allowlist with --allow-env=FOO,BAR. The expectation is that a program running without env permission cannot change process.env. process.loadEnvFile() (the Node-compatible API for loading variables from a .env file) does not honor this. It only checks that the program has read permission for the dotenv file, then writes every key in that file into the process environment — even when env access is denied. In effect, --allow-read plus a writable or attacker-controlled .env file is enough to defeat --deny-env. This vulnerability is fixed in 2.8.1.	5.2	More Details

CVE-2026-49860	Deno is a JavaScript, TypeScript, and WebAssembly runtime. Prior to 2.8.1, when a WebSocket connection was opened, Deno checked the destination hostname against --deny-net rules but did not re-check the IP addresses that hostname resolved to. An attacker-controlled script could use a specially crafted domain name that passes the hostname check yet resolves to a denied IP, bypassing the network restriction entirely. This vulnerability is fixed in 2.8.1.	5.2	More Details
CVE-2026-49859	Deno is a JavaScript, TypeScript, and WebAssembly runtime. Prior to 2.8.1, when fetch() was called, Deno checked the destination hostname against --deny-net rules but did not re-check the IP addresses that hostname resolved to. An attacker-controlled script could use a specially crafted domain name that passes the hostname check yet resolves to a denied IP, bypassing the network restriction entirely. This vulnerability is fixed in 2.8.1.	5.2	More Details
CVE-2026-55443	LangChain is a framework for building agents and LLM-powered applications. Prior to 1.3.9, several LangChain components that resolve filesystem paths or expand search patterns do not consistently confine the resolved path to the intended root directory. Affected behaviors include: a file-search agent middleware that validates a starting directory but not the search pattern or the resolved target of matched files, so glob patterns and symlinks can reach files outside the configured root; prompt- and chain/agent-configuration loaders that accept path fields and resolve them without confining the result to a trusted base or rejecting symlink targets; and path-prefix authorization checks that compare by string prefix without a path-segment boundary, so a sibling path sharing the prefix is accepted. When these components receive path values, search patterns, or workspace contents influenced by an untrusted source — including an LLM acting on untrusted input — the result can be disclosure of files outside the intended boundary. This vulnerability is fixed in 1.3.9.	5.1	More Details
CVE-2026-11791	A flaw was found in 389 Directory Server. During schema reload, the attr_syntax_swap_ht() function unconditionally frees attribute syntax information nodes, bypassing the refcount-based deferred deletion used elsewhere in the attribute syntax subsystem. If an administrator triggers schema reload while concurrent LDAP query traffic is active, worker threads may access freed memory, resulting in use-after-free or double-free and a denial of service (server crash).	5.0	More Details
CVE-2026-55655	A flaw was found in OpenSSH. A local unprivileged attacker on a Linux client host can hijack client-side X11 forwarding connections. This is possible by pre-binding the preferred abstract X socket name when X11 forwarding is enabled and a local UNIX-domain X socket is used. A successful attack can compromise the confidentiality of forwarded X11 traffic, including sensitive window contents and input, and may allow some manipulation of the forwarded session.	5.0	More Details
CVE-2026-12771	A vulnerability was identified in BerriAI litellm up to 1.82.2. This affects an unknown function of the file litellm/proxy/auth/user_api_key_auth.py of the component M2M JWT Handler. Such manipulation leads to improper authorization. The attack can be launched remotely. A high complexity level is associated with this attack. The exploitability is reported as difficult. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure.	5.0	More Details
CVE-2026-7547	The Woosa – Marktplaats for WooCommerce plugin for WordPress is vulnerable to Arbitrary File Read via Path Traversal in versions up to and including 2.0.4. This is due to insufficient path sanitization in the render_logs_ui() function, which accepts a base64-encoded file name from the 'log_file' GET parameter and concatenates it directly with the plugin's log directory path without validating that the resolved path remains within the intended directory. This makes it possible for authenticated attackers, with Administrator-level access, to read the contents of arbitrary files on the server, including wp-config.	4.9	More Details
CVE-2026-56131	libexpat before 2.8.2 lacks handler call depth tracking for calls to XML_ResumeParser from within handlers in cases of a policy violation. Thus, a use-after-free can occur (similar to the CVE-2026-50219 situation).	4.9	More Details
CVE-2026-56080	Capgo before 12.128.2 contains a flaw in the Enforce Password Policy feature: after a Super Admin enables the policy and successfully changes their password to a compliant one, the backend does not update the password-compliance state. As a result, the backend continues to treat the account as non-compliant and repeatedly forces password-reset prompts, permanently locking the Super Admin out of organization access (organization lockout / denial of service) despite valid authentication.	4.9	More Details
	The Tutor LMS – eLearning and online course solution plugin for WordPress is vulnerable to generic SQL Injection via the 'data' parameter in all versions up to, and including, 3.9.11 due to		

CVE-2026-10736	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-2026-56228	Capgo before 12.128.2 fails to enforce a maximum value on the minimum password length field in its password policy configuration. An authenticated organization administrator can set an extremely large numeric value (e.g., billions of characters) as the minimum password length, making compliance impossible for all organization members. Once the policy is enabled, users (including administrators) are unable to change their passwords or access the organization, resulting in an organization-wide account lockout and application-level denial of service.	4.9	More Details
CVE-2026-11776	The Form Maker by 10Web – Mobile-Friendly Drag & Drop Contact Form Builder plugin for WordPress is vulnerable to generic SQL Injection via the 'groupids' parameter in all versions up to, and including, 1.15.43 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-2026-56412	libexpat before 2.8.2 does not consider XML_TOK_DATA_CHARS in doCdataSection and thus lacks handler call depth tracking for various calls from within handlers in cases of a policy violation. Thus, a use-after-free can occur. NOTE: this issue exists because of an incomplete fix for CVE-2026-50219.	4.9	More Details
CVE-2026-10645	Zephyr's ext2 directory-entry parser does not fully validate on-disk directory entry structure before copying the entry name and advancing traversal state. In ext2_fetch_direntry() (subsys/fs/ext2/ext2_diskops.c), the code only checks de_name_len <= EXT2_MAX_FILE_NAME and then copies the name with memcpy without validating the structural relationship between de_rec_len, de_name_len, and the directory block boundary (for example that de_rec_len is non-zero, at least the size of the entry header, and that the record fits within the block). Callers such as find_dir_entry() and ext2_get_direntry() (subsys/fs/ext2/ext2_impl.c) then advance traversal using the unvalidated de_rec_len. A crafted ext2 image can therefore cause an out-of-bounds read from the directory block buffer when a malformed entry near the end of a block triggers an oversized name copy, or a zero-progress infinite loop when de_rec_len == 0. The issue is not reached at mount time but later through directory traversal paths such as pathname lookup, stat/open/unlink/rename, and readdir. The primary impact is denial of service and out-of-bounds reads under attacker-controlled ext2 images mounted from untrusted media.	4.9	More Details
CVE-2026-41280	Incorrect Authorization vulnerability allows users with system login privileges to delete task definitions in unauthorized projects This issue affects Apache DolphinScheduler versions prior to 3.4.2. Users are recommended to upgrade to version 3.4.2, which fixes this issue.	4.9	More Details
CVE-2026-11777	The Form Maker by 10Web – Mobile-Friendly Drag & Drop Contact Form Builder plugin for WordPress is vulnerable to generic SQL Injection via the 'name' parameter in all versions up to, and including, 1.15.43 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, 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-2026-11360	The Advanced Order Export For WooCommerce plugin for WordPress is vulnerable to generic SQL Injection via the 'sort_direction' parameter in all versions up to, and including, 4.0.10 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with shop manager-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. The endpoint requires a valid woe_nonce and Shop Manager-level capabilities (view_woocommerce_reports or export_woocommerce_orders), and wp_magic_quotes protection is stripped via stripslashes_deep() before processing, allowing quote and backslash characters to survive intact into the SQL context.	4.9	More Details
CVE-2026-	Postiz is an AI social media scheduling tool. Versions prior to 2.21.8 contained an unauthenticated endpoint that accepted a signed token and applied subscription-enforcement side effects to the organization referenced in that token's claims, without verifying the token's intended purpose. The endpoint, /public/modify-subscription, could not change the persisted subscription tier, but it did execute enforcement-related side effects on the caller's own	4.8	More

48783	organization, including adjusting team-member enablement state, disabling integrations exceeding the asserted plan's limits, and resetting the scheduled-post cron when the asserted plan was the free tier. Impact is limited to the attacker's own organization and cannot be redirected at other tenants through this endpoint. This issue has been fixed in version 2.21.8.		Details
CVE-2026-55766	guzzlehttp/psr7 is a PSR-7 HTTP message library implementation in PHP. Prior to 2.12.1, guzzlehttp/psr7 did not reject CR/LF characters in certain first-party HTTP start-line fields: the request method, protocol version, and response reason phrase. If an application placed attacker-controlled data into one of those fields and later serialized the PSR-7 message as raw HTTP/1.x, for example with Message::toString() or an equivalent serializer, the serialized message could contain attacker-controlled header lines. The issue can also be reached through Message::parseRequest() or Message::parseResponse() when malformed raw messages are parsed into first-party PSR-7 objects and then serialized again. Creating or modifying a Request, Response, or other PSR-7 object alone is not sufficient. The issue requires the malformed message to be serialized and written to the network, forwarded, replayed, or otherwise processed by software that does not independently reject the malformed start line. This vulnerability is fixed in 2.12.1.	4.8	More Details
CVE-2026-56381	Craft CMS from version 5.0.0-RC1 contains a stored cross-site scripting vulnerability in the User Permissions page where user group names are rendered without proper HTML escaping. Attackers with admin access can inject arbitrary JavaScript via the user group name field that executes when other users view or edit permissions.	4.8	More Details
CVE-2026-56383	Craft CMS contains a stored cross-site scripting (XSS) vulnerability in the editableTable.twig component when using the 'Row Heading' column type. The application fails to sanitize input within row heading default values, allowing an attacker with an administrator account (with allowAdminChanges enabled) to inject arbitrary JavaScript that executes when another user views a page containing the affected table field. Affected versions are >= 4.5.0-beta.1 through 4.16.18 and >= 5.0.0-RC1 through 5.8.22; fixed in 4.16.19 and 5.8.23.	4.8	More Details
CVE-2026-54289	Hono is a Web application framework that provides support for any JavaScript runtime. Prior to 4.12.25, on AWS Lambda@Edge, CloudFront delivers a request header that appears more than once as several separate entries. The adapter writes each value with Headers.set instead of Headers.append, so every value overwrites the previous one and only the last reaches the application. Repeated request headers such as X-Forwarded-For, Forwarded, and Via are silently truncated to a single value. Request middleware sees only the last value of a repeated header instead of the full chain. For applications that base access control on the X-Forwarded-For chain, this can weaken or alter that decision; for auditing, hop history is lost. This vulnerability is fixed in 4.12.25.	4.8	More Details
CVE-2026-56393	Craft CMS 4.x (>= 4.0.0-RC1, < 4.17.0-beta.1) and 5.x (>= 5.0.0-RC1, < 5.9.0-beta.1) contain multiple stored cross-site scripting vulnerabilities where settings names and field option labels are rendered without sanitization (e.g., via the checkbox.twig template, which used {{ label|raw }}). An authenticated administrator (with allowAdminChanges enabled) can inject malicious payloads into section names, volume names, user group names, global set names, generated field names, checkbox/radio option labels, and custom source labels, causing arbitrary JavaScript to execute in other users' control-panel sessions. Fixed in 4.17.0-beta.1 and 5.9.0-beta.1.	4.8	More Details
CVE-2026-12491	A flaw was found in vLLM, an open-source library for large language model inference. This vulnerability arises from improper handling of image metadata, specifically EXIF orientation and PNG transparency (tRNS) data, during image processing. When images are converted to RGB, transparency information may be implicitly discarded or remapped, leading to unexpected rendering of transparent pixels and distortion of input content. This can result in the model misinterpreting image content, potentially affecting the integrity of processed data.	4.8	More Details
CVE-2026-48823	Shaarli is a personal bookmarking service. Versions 0.16.1 and prior contain a stored Cross-Site Scripting (XSS) vulnerability in the tag filtering functionality of Shaarli. An authenticated user can inject arbitrary JavaScript into the tags field when creating a bookmark (Shaare). The malicious payload is stored and later executed when users interact with the "Filter by tag" search feature on the homepage. User-supplied input in the tags field is not properly sanitized or output-escaped before being rendered in the tag filtering interface. When a bookmark is created with a malicious payload inside the tag field, the payload is stored in the database. Later, when a user searches using the "Filter by tag" functionality on the homepage, the application renders matching tags dynamically. If the tag value contains HTML with JavaScript event handlers, it is	4.8	More Details

	injected into the DOM. This impacts anyone interacting with the "Filter by tag" search functionality, administrators and privileged users. This issue has been fixed in version 0.16.2.		
CVE-2026-22674	Hashgraph Guardian through 3.6.0, fixed in commit ba8c566, contains a stored cross-site scripting vulnerability that allows authenticated users with the STANDARD_REGISTRY role to inject malicious scripts by submitting a crafted companyName value via the branding configuration API endpoint. Attackers can exploit the unsanitized innerHTML assignment in the branding service to execute arbitrary JavaScript in the browser of every authenticated user on every page load.	4.8	More Details
CVE-2026-56294	capacitor-native-biometric before 12.128.2 contains an authentication bypass vulnerability where the onAuthenticationSucceeded() method fails to validate CryptoObject parameters. Attackers can hook the onAuthenticationSucceeded() function using dynamic instrumentation to bypass biometric authentication without valid credentials.	4.8	More Details
CVE-2026-40641	Dell PowerFlex Manager, version(s) 4.6.0.1, contain(s) an Use of a Broken or Risky Cryptographic Algorithm vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Information disclosure and Information tampering.	4.8	More Details
CVE-2026-48142	NGINX Plus and NGINX Open Source have a vulnerability in the ngx_http_charset_module module. When content is served or proxied through a location block with both source_charset utf-8; and a charset directive (for example, charset koi8-r;) configured, remote, unauthenticated attackers can send requests (in conjunction with conditions beyond their control) to cause a heap buffer over-read in the NGINX worker process, leading to limited disclosure of memory or a restart. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	4.8	More Details
CVE-2026-12549	The fix for CVE-2026-2443 was regressed by a subsequent rework commit that replaced specific overflow checks with a general signed comparison. When a client sends a Range request with a suffix length exceeding the content size, the resulting negative start value is not properly clamped, leading to malformed HTTP 206 responses and log flooding.	4.8	More Details
CVE-2026-46772	Vulnerability in the Oracle Application Development Framework (ADF) product of Oracle Fusion Middleware (component: ADF Faces). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Application Development Framework (ADF) executes to compromise Oracle Application Development Framework (ADF). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Application Development Framework (ADF) accessible data as well as unauthorized update, insert or delete access to some of Oracle Application Development Framework (ADF) accessible data. CVSS 3.1 Base Score 4.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:L/A:N).	4.7	More Details
CVE-2026-56117	dhcpcd through 10.3.2, fixed in commit 78ea09e, contains a heap use-after-free vulnerability in the control socket handling within src/control.c that allows local unprivileged attackers to trigger memory corruption when privilege separation is disabled. Attackers can connect to the control socket and send a privileged command such as -x, causing control_recvdata() to free the client object while the same READ+HANGUP event subsequently reaches control_hangup() with the stale pointer, resulting in a use-after-free condition exploitable in deployments using --disable-privsep or where privsep initialization has failed with the control socket operating in mode 0666.	4.7	More Details
CVE-2026-12463	Inappropriate implementation in Views in Google Chrome on Linux prior to 149.0.7827.155 allowed a remote attacker who had compromised the renderer process to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: High)	4.7	More Details
CVE-2026-48986	pam_usb provides hardware authentication for Linux using removable media. In pam_usb 0.9.1 and earlier, usb_get_process_parent_id() can cause an infinite loop DoS because it does not initialize *ppid on failure. In pusb_local_login(), the same variable is reused as input and output in a process-tree while loop; if /proc/<pid>/stat cannot be read (for example, when an ancestor process exits during authentication), the PID is not updated and the loop does not terminate. This hangs the authenticating process (such as sudo, sshd, or login) until it is forcibly terminated. This issue has been fixed in version 0.9.2.	4.7	More Details
CVE-2026-	Capgo before 12.128.2 contains an open redirect vulnerability in the confirm-signup endpoint that allows attackers to redirect users to arbitrary external websites. The confirmation_url parameter is not validated, enabling attackers to craft malicious links for phishing and credential	4.7	More Details

56332	harvesting attacks.		
CVE-2026-48984	pam_usb provides hardware authentication for Linux using ordinary removable media. In versions 0.9.1 and below, the xfree() memory release helper in calls free() without first zeroing the buffer contents, releasing heap-allocated buffers containing sensitive data — including one-time pad bytes read from disk — without clearing, leaving the sensitive content in freed heap memory until it happens to be overwritten by a subsequent allocation. On a system where a use-after-free condition exists, or where a heap inspection primitive becomes available, this could allow recovery of pad values or other authentication material from freed memory regions. This is a defence-in-depth requirement consistent with prior hardening work in this codebase (GHSA-vx6f-rrqr-j87c applied explicit_bzero to some pad paths; this issue generalises the pattern to the central deallocation helper).	4.7	More Details
CVE-2026-54106	The U.S. Government Accountability Office (GAO) Electronic Protest Docketing System (EPDS) and Civilian Board of Contract Appeals (CBCA) Electronic Docketing System (EDS) do not validate X-Forwarded-For HTTP headers, allowing a remote attacker with compromised administrator credentials to bypass network access controls and log in.	4.7	More Details
CVE-2026-50267	Steeltoe is an open source project that provides a collection of libraries that helps users build cloud-native applications. In Steeltoe.Configuration.Abstractions 4.0.0 through 4.1.0, when MySQL or PostgreSQL service bindings from `VCAP_SERVICES` include TLS client credentials, the Connectors library writes those credentials to temporary files in `Path.GetTempPath()` using `File.CreateText`. On Linux, `File.CreateText` creates files with mode `0644` (world-readable) under the process umask, and the files are never deleted. The same key material is protected at mode `0400` in `/proc/<pid>/environ`. Steeltoe.Configuration.Abstractions version 4.2.0 patches the issue. If an immediate upgrade is not possible, prevent other processes from running in the container under a different UID with access to `/tmp`.	4.7	More Details
CVE-2026-44587	CarrierWave is a framework to upload files from Ruby applications. In versions prior to 2.2.7 and 3.1.3, the content_type_denylist check fails to escape regex metacharacters in string entries, causing the denylist to silently not match the content types it is intended to block. In lib/carrierwave/uploader/content_type_denylist.rb:57, denylist entries are interpolated directly into a regex without Regexp.quote or anchoring, so an entry such as image/svg+xml becomes the pattern /image\/svg+xml/, in which + is treated as a quantifier rather than a literal character and therefore never matches the real MIME type image/svg+xml. This is inconsistent with the allowlist implementation, which correctly applies both Regexp.quote and a \A anchor. Other content types containing regex metacharacters, such as application/xhtml+xml, are affected as well. As a result, any application that relies on content_type_denylist to block image/svg+xml, most commonly to prevent stored XSS, is silently unprotected. An attacker can upload an SVG file containing arbitrary JavaScript; if the application serves that SVG inline from its own origin, the script executes in the victim's browser, resulting in stored XSS. This issue has been fixed in versions 2.2.7 and 3.1.3.	4.7	More Details
CVE-2026-39595	Author Broken Access Control in W3 Total Cache <= 2.9.1 versions.	4.7	More Details
CVE-2026-12789	A vulnerability was identified in ILIAS Learning Management System 11.0. This issue affects the function ilTrQuery::executeQueries of the file components/ILIAS/Tracking/classes/class.ilTrQuery.php of the component Learning Progress Tracking. Such manipulation of the argument troup_table_nav leads to sql injection. It is possible to launch the attack remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2026-11358	The Orbit Fox: Duplicate Page, Menu Icons, SVG Support, Cookie Notice, Custom Fonts & More plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 3.0.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, 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
	A flaw was found in GStreamer's gst-plugins-bad package. When processing a specially crafted H.264 video file containing malformed MVC or SVC extension slice NAL units, a 1-byte heap out-		

CVE-2026-12892	of-bounds read can occur during parsing. This happens when the parser attempts to check slice boundary information without first verifying that the NAL unit contains enough data beyond the extension header. An attacker could exploit this by tricking a user into opening a malicious H.264 video file, potentially causing the application to crash or leak a single byte of heap memory.	4.4	More Details
CVE-2025-13162	Uncontrolled Search Path Element vulnerability in ABB Control Builder A, ABB 800xA for Advant Master. This issue affects Control Builder A: through 1.4/4; 800xA for Advant Master: through 6.0.3-1, through 6.1.1-1, 6.1.1-3, 6.2.0-1.	4.4	More Details
CVE-2026-12164	Fortra File Integrity Monitoring (FIM), formerly Tripwire Enterprise, versions prior to 9.4.0 may assign incorrect or elevated effective permissions to users created by the tetool import command while FIM is running, particularly when the import also creates or changes roles or role-permission relationships.	4.4	More Details
CVE-2026-54325	Pi is a minimal terminal coding harness. Pi before 0.79.0 loaded project-local configuration and resources from a repository's .pi directory without first asking the user to trust that repository. This included project-local extensions, which are executable TypeScript or JavaScript modules loaded into the Pi process. An attacker who controls a repository could place Pi-specific project resources in that repository. If a user then started Pi from that working tree, the project-local extension code could run with the same privileges as the local Pi process without the user having a convenient way to make a trust decision. This vulnerability is fixed in 0.79.0.	4.4	More Details
CVE-2026-12430	The Blocksy Companion plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 2.1.45 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with editor-level permissions and above, 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-2026-9013	The Bogo plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.9.1 via the bogo_rest_create_post_translation. This makes it possible for authenticated attackers, with subscriber-level access and above, to extract the raw title, content, excerpt, and password of any private, draft, or password-protected post by triggering its duplication via the translation endpoint and reading the returned title.raw, content.raw, and excerpt.raw fields of the duplicated post. This vulnerability is exploitable against posts written in a non-default locale, as authenticated subscribers can request a translation into the site's default locale to pass the locale-only permission gate. While subscribers can trigger the endpoint, this is only impactful at the Contributor-level as they can actually read the duplicated content.	4.3	More Details
CVE-2026-56255	Capgo before 12.128.2 contains a denial of service vulnerability in the POST /app/demo endpoint that allows authenticated users with org write permissions to create unlimited demo applications without rate limiting or quota enforcement. Attackers can repeatedly invoke this endpoint to generate approximately 138 database write operations per request, causing degraded performance, increased costs, and potential service instability.	4.3	More Details
CVE-2026-54006	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.6, POST /api/v1/calendars/events/{event_id}/update validates that the caller has write access to the calendar the event currently belongs to, but does not validate the destination calendar_id supplied in the request body. The model layer then persists the new calendar_id unconditionally. A regular user-role account can therefore create an event in their own calendar and immediately move it into any other user's calendar whose ID they know — bypassing the authorization check that create_event correctly performs. This vulnerability is fixed in 0.9.6.	4.3	More Details
CVE-2026-10779	The Classified Listing – Classified ads & Business Directory plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 5.4.2. This is due to a missing capability/ownership check on the gallery_image_update_as_feature AJAX handler (action: rtcl_fb_gallery_image_update_as_feature), which accepts a user-supplied listing ID and attachment ID and sets the featured image of a listing while only validating a nonce that is exposed to any logged-in user on the frontend listing-submission form. This makes it possible for authenticated attackers, with Subscriber-level access and above, to change the featured image of arbitrary listings they do not own.	4.3	More Details

CVE-2026-12804	A vulnerability was detected in lemonldap-ng up to 2.23.0. Impacted is an unknown function in the library lemonldap-ng-portal/lib/Lemonldap/NG/Portal/CDC.pm of the component SAML Common Domain Cookie Endpoint. Performing a manipulation of the argument url results in open redirect. The attack is possible to be carried out remotely. The exploit is now public and may be used. Applying a patch is the recommended action to fix this issue. The vendor confirms, that "it has been fixed some days ago and will be available in 2.23.1. CDC is quite never used, so the impact is very low."	4.3	More Details
CVE-2026-54014	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.6, a path traversal vulnerability exists in open-webui's cache file serving endpoint that allows any authenticated user to read files from sibling directories outside the intended cache directory, by exploiting an incomplete startswith containment check that lacks a trailing path separator. The root cause is that serve_cache_file() in open_webui/main.py validates the resolved path with file_path.startswith(os.path.abspath(CACHE_DIR)) — without appending os.sep. This allows any path resolving to a sibling directory whose name begins with cache (e.g. cache_sibling, cache_backup, cached_models) to pass validation. This vulnerability is fixed in 0.9.6.	4.3	More Details
CVE-2026-54016	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.6, Open WebUI has a Broken Object Level Authorization (BOLA) vulnerability in the builtin search_knowledge_files tool. When native function calling is enabled and the selected model has no attached knowledge bases, an authenticated user can call search_knowledge_files with an arbitrary knowledge_id. The function then returns file metadata from that knowledge base without checking whether the user has read access. This allows unauthorized enumeration of private or restricted knowledge base files. This vulnerability is fixed in 0.9.6.	4.3	More Details
CVE-2024-33685	Missing Authorization vulnerability in Jegstudio Startupzy startupzy allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Startupzy: from n/a through 1.1.1.	4.3	More Details
CVE-2026-55517	Deno is a JavaScript, TypeScript, and WebAssembly runtime. Prior to 2.7.5, a Deno program that opens a client WebSocket connection could be crashed by the remote server. While handling the WebSocket handshake response, Deno parsed the Sec-WebSocket-Protocol and Sec-WebSocket-Extensions response headers in a way that assumed their bytes were always printable ASCII. A response header containing non-visible-ASCII bytes (0x80-0xFF) caused a panic that aborted the entire Deno process. This vulnerability is fixed in 2.7.5.	4.3	More Details
CVE-2026-20178	A vulnerability in the browser-based version of Cisco Webex App could have allowed an unauthenticated, remote attacker to redirect users to a malicious webpage. Cisco has addressed this vulnerability in the Cisco Webex App, and no customer action is needed. This vulnerability existed due to improper input validation of URL parameters in an HTTP request. Prior to this vulnerability being addressed, an attacker could have exploited this vulnerability by persuading a user to click a crafted URL. A successful exploit could have allowed the attacker to redirect a user to a malicious website.	4.3	More Details
CVE-2026-12515	A flaw was found in Katello's of Red Hat Satellite. A content upload functionality where insufficient authorization checks in the ContentUploadsController allowed users with the edit_products permission to query content information for repositories outside the products they were authorized to manage. An authenticated attacker could exploit this issue to determine whether specific content exists within repositories that should otherwise be inaccessible. This issue does not allow unauthorized modification, import, or publication of content.	4.3	More Details
CVE-2026-49337	libde265 is an open source implementation of the h.265 video codec. Prior to version 1.0.20, a crafted sequence of H.265 NAL units causes `decoder_context::read_slice_NAL()` (`libde265/decctx.cc:481`) to attach slice headers to a finished picture object that has no active image unit, resulting in attacker-controlled unbounded heap growth. The retained headers are never freed until the picture is released, which may not happen during continuous streaming. Version 1.0.20 patches the issue.	4.3	More Details
CVE-2026-	The Equalize Digital Accessibility Checker – WCAG, ADA, EAA and Section 508 compliance plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.42.1. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with author-level access and above, to dismiss, ignore, or restore accessibility audit issue records belonging to posts they are not permitted to edit by supplying an issue from their own post as an authorization token to affect	4.3	More Details

9199	matching issues across the entire site. An Author-level user can exploit this by passing largeBatch=true on a dismiss-issue request referencing one of their own post's issues, causing the handler to bulk-modify all site-wide accessibility issues sharing the same 'object' value — including those belonging to administrator-owned posts.		
CVE-2026-12469	Uninitialized Use in GPU in Google Chrome on Android prior to 149.0.7827.155 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2026-9162	Mattermost versions 11.7.x <= 11.7.0, 11.6.x <= 11.6.2, 11.5.x <= 11.5.5, 10.11.x <= 10.11.17 fail to invalidate cached authentication state for active WebSocket connections during global session revocation, which allows a user with an existing WebSocket connection to remain authenticated and continue receiving real-time events until the cached session expires or the client reconnects.. Mattermost Advisory ID: MMSA-2026-00664	4.3	More Details
CVE-2025-32748	Dell PowerFlex rack, version(s) RCM 3.7/3.7, contain(s) a Host Header Injection vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability to trigger redirections.	4.3	More Details
CVE-2026-12891	A flaw was found in the GStreamer gst-plugins-bad package. When processing a malformed H.266/VVC video stream with a crafted aspect ratio indicator value, the H.266 parser performs an out-of-bounds read of up to 8 bytes from adjacent memory. This flaw allows an attacker to craft a malicious H.266 video file or stream that, when processed by a GStreamer-based application, could leak limited memory contents through video metadata, potentially exposing sensitive information from the application's address space.	4.3	More Details
CVE-2026-11784	The Optimole – Optimize Images | Convert WebP & AVIF | CDN & Lazy Load | Image Optimization plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 4.2.6. This is due to missing or incorrect nonce validation on the replace_file function. This makes it possible for unauthenticated attackers to overwrite existing media attachments with attacker-supplied file content by supplying a forged multipart POST request targeting any attachment the victim has edit_post capability over via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. The forged request requires a victim with at least Author-level privileges, as the handler enforces a current_user_can('edit_post', $id) check; tricking an Author-level or higher user into clicking a crafted link is sufficient to trigger the overwrite against attachments that user can edit.	4.3	More Details
CVE-2026-12050	SQL injection in pgAdmin 4's named restore point endpoint (POST /browser/server/restore_point/{gid}/{sid}). The user-supplied 'value' field was interpolated directly into the SQL string with str.format() instead of being passed as a bound parameter, allowing an authenticated pgAdmin user with a connected PostgreSQL session to inject additional statements through that endpoint. The injected SQL executes under the database role the user is already authenticated as. The defect does not cross a privilege boundary -- the user already has direct SQL access to that role through the Query Tool -- so the attacker gains no capability beyond what their database role already grants them. The marginal impact accounts for the fact that the injection path is not the documented SQL-execution interface, so a deployment that gates the Query Tool at the application layer could see SQL executed through a path it did not anticipate. Fix passes the restore point name as a bound parameter and schema-qualifies the function call as pg_catalog.pg_create_restore_point so a non-default search_path on the connection cannot redirect the call to a shadow definition. A regression test asserts the value arrives as a bound parameter and not spliced into the SQL string. This issue affects pgAdmin 4: from 1.0 before 9.16.	4.3	More Details
CVE-2026-11775	The User Admin Simplifier plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.0.0. This is due to missing or incorrect nonce validation on the useradminsimplifier_options_page function. This makes it possible for unauthenticated attackers to reset and permanently delete any user's stored menu and admin-bar configuration via a forged request that triggers uas_save_admin_options() and overwrites the useradminsimplifier_options database entry 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-2026-24575	Subscriber Broken Access Control in WishList Member X <= 3.29.0 versions.	4.3	More Details

CVE-2024-24709	Missing Authorization vulnerability in Shareaholic allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Shareaholic: from n/a through 9.7.11.	4.3	More Details
CVE-2025-71379	vLLM versions >= 0.6.3 and < 0.9.0 contain multiple regular expression denial of service (ReDoS) vulnerabilities. Several regex patterns — in vllm/lora/utils.py, the phi4mini tool parser, and the OpenAI-compatible serving chat endpoint — are susceptible to catastrophic backtracking. An attacker submitting crafted input with nested or repeated structures can trigger severe CPU consumption and performance degradation, resulting in denial of service.	4.3	More Details
CVE-2026-10623	The PressPrimer Quiz – AI Quiz Maker, Exam Builder & LMS Assessment Plugin plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 2.3.0 via the 'rule_id' parameter due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with custom-level access and above, to modify or delete quiz rules belonging to other teachers, resulting in unauthorized tampering of another user's quiz structure.	4.3	More Details
CVE-2024-31435	: Missing Authorization vulnerability in Inisev Social Media & Share Icons allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Social Media & Share Icons: from n/a through 2.8.6.	4.3	More Details
CVE-2026-11357	The Kadence Blocks — Page Builder Toolkit for Gutenberg Editor plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.7.5 via the editor_assets_variables. This makes it possible for authenticated attackers, with contributor-level access and above, to extract the site's connected Kadence account license key, license owner email, api_key, api_email, and license domain from the browser console by inspecting window.kadence_blocks_params.proData. Exploitation requires only that an administrator has previously connected a valid Kadence license; the full credential bundle is then readable by any Contributor-level user from the block editor client context without any server-side request manipulation.	4.3	More Details
CVE-2026-10023	The Dokan: AI Powered WooCommerce Multivendor Marketplace Solution – Build Your Own Amazon, eBay, Etsy plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 5.0.3 via the change_order_status, add_order_note, delete_order_note, add_shipping_tracking_info, grant_access_to_download, and revoke_access_to_download AJAX handlers due to missing ownership validation on a user-controlled order ID key. This makes it possible for authenticated attackers, with custom vendor-level access and above, to modify the status of arbitrary orders, add attacker-controlled notes to any order (including customer-facing notes that trigger WooCommerce notification emails to buyers), delete any order note or WordPress comment by ID regardless of ownership, inject fake shipping tracking information on any order, and grant or revoke downloadable-product permissions on any order in the marketplace. Critically, nonce validity is not a barrier to exploitation: each of these AJAX handlers generates and embeds its nonce on the authenticated vendor's own dashboard order pages (e.g., /dashboard/orders/?order_id=OWN_ORDER_ID), which the attacker legitimately controls. The attacker harvests a valid nonce from their own order detail page and replays it against a victim order ID — the nonce only proves the request originates from a logged-in session, not that the order belongs to that vendor. This directly rebuts the prior rejection reasoning that 'users cannot generate valid nonces on command': vendor users can and do generate valid nonces on demand simply by loading their own dashboard pages. Source-code analysis confirmed the vulnerable code path is present and unpatched through version 5.0.1.	4.3	More Details
CVE-2024-34810	Cross-Site request forgery (CSRF) vulnerability in Extend Themes Skyline WP allows Cross Site Request Forgery. This issue affects Skyline WP: from n/a through 1.0.10.	4.3	More Details
CVE-2024-35648	Cross-Site request forgery (CSRF) vulnerability in Andy Moyle Emergency Password Reset allows Cross Site Request Forgery. This issue affects Emergency Password Reset: from n/a through 8.0.	4.3	More Details
CVE-2024-37496	Missing Authorization vulnerability in Rara Themes Metro Magazine allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Metro Magazine: from n/a through 1.3.7.	4.3	More Details
CVE-	In Splunk AI Toolkit versions below 5.7.4, a low-privileged user that does not hold the "admin" or "power" Splunk roles could cause the Splunk AI Toolkit to make outbound requests over HTTP to		

2026-20265	a server that an attacker controls, which could allow for data exfiltration. The vulnerability exists because of an insecure default domain allowlist in the Splunk AI Toolkit, which does not restrict outbound AI agent requests to approved external domains.	4.3	More Details
CVE-2025-48571	In multiple functions of btm_sec.cc, there is a possible way for an attacker to intercept SMS messages due to a logic error in the code. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.	4.3	More Details
CVE-2026-12811	A weakness has been identified in kortix-ai suna up to 0.8.38. Affected by this issue is the function router.replace/router.push of the file apps/frontend/src/app/auth/page.tsx of the component Auth Endpoint. Executing a manipulation of the argument returnURL can lead to cross site scripting. The attack may be launched remotely. The exploit has been made available to the public and could be used for attacks. Upgrading to version 0.8.39 can resolve this issue. This patch is called f5dec7aa0c1b8fa0125938f292c0f2430ca75f6c. It is advisable to upgrade the affected component. The researcher explains: "The issue was fixed in v0.8.39 without notifying the wider user base via a security disclosure."	4.3	More Details
CVE-2025-59872	HCL ZIE for Web is affetced by an Unrestricted File Upload vulnerability, If the server is configured to execute code, then it may be possible to obtain command execution on the server by uploading a file known as a web shell, which allows you to execute arbitrary code or operating system commands. For this attack to be successful, the file needs to be uploaded inside the Webroot, and the server must be configured to execute the code	4.3	More Details
CVE-2026-56319	Capgo before 12.128.2 contains an information disclosure vulnerability in the GET /statistics/app/:app_id endpoint that allows app-limited API keys to distinguish existing sibling app IDs through differential error responses. Attackers can enumerate real app IDs outside their allowed scope by observing 500 PGRST116 errors for inaccessible apps versus 401 errors for nonexistent apps, breaking tenant isolation.	4.3	More Details
CVE-2026-12799	A security vulnerability has been detected in BerriAI litellm up to 1.82.2. Affected by this issue is the function ui_view_users of the file litellm/proxy/management_endpoints/internal_user_endpoints.py of the component Incomplete Fix CVE-2025-0628. Such manipulation leads to improper authorization. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure.	4.3	More Details
CVE-2026-40723	Subscriber Broken Access Control in Bricks Builder <= 2.1.4 versions.	4.3	More Details
CVE-2026-55653	A flaw was found in OpenSSH. A malicious SSH server can exploit a double free vulnerability in the Diffie-Hellman Group Exchange (DH-GEX) client path. This occurs during FIPS (Federal Information Processing Standards) mode known-group validation when the client processes attacker-controlled DH-GEX group parameters. Successful exploitation leads to client-side process termination, resulting in a Denial of Service (DoS).	4.3	More Details
CVE-2026-56307	Cap-go before 12.128.12 contains a broken cursor pagination vulnerability in the /private/devices endpoint on the Cloudflare/workerd path that allows authenticated attackers to cause duplicate-page loops and make later rows unreachable. Attackers with app.read_devices access can exploit non-advancing cursor filters to trigger infinite pagination loops, prevent dataset traversal, and cause repeated processing in device-management workflows.	4.3	More Details
CVE-2026-12049	Open redirect in pgAdmin 4's multi-factor authentication flow. The MFA validate and register endpoints honoured the user-supplied 'next' query/form parameter without confirming the target pointed back inside pgAdmin, so an authenticated victim who clicked /mfa/validate?next=<external> -- a link typically delivered by phishing -- would be sent to an attacker-controlled host directly out of the trusted auth flow. The defect is a trusted-domain redirect, not a privilege bypass: the attacker gains no read/write access to pgAdmin or the victim's database, but the redirect launders the attacker's destination through pgAdmin's URL, which raises the success rate of credential-phishing follow-on against the victim. Fix introduces a same-origin _is_safe_redirect_url helper and gates every MFA redirect that consumes user-supplied 'next' values through it. The helper allows only relative paths and absolute URLs whose scheme is http(s) and whose host matches the current request host; it rejects external hosts in absolute and protocol-relative form, non-http schemes (javascript:, data:, mailto:), userinfo tricks (http://localhost@attacker/), and backslash variants that some browsers normalize to forward	4.3	More Details

	slashes. Unsafe targets fall back to the internal browser index. A dedicated regression test exercises each accept/reject category and the original reporter PoC. This issue affects pgAdmin 4: from 6.0 before 9.16.		
CVE-2026-46548	NocoDB is software for building databases as spreadsheets. Prior to 2026.04.1, the request-filtering-agent SSRF protection was non-functional in the four notification webhook plugins (Slack, Discord, Mattermost, Teams) because httpAgent / httpsAgent were passed as part of the request body rather than the axios config. An authenticated user with hook-creation permission could direct outbound POST requests to arbitrary internal hosts. This vulnerability is fixed in 2026.04.1.	4.3	More Details
CVE-2026-12446	Inappropriate implementation in Passwords in Google Chrome prior to 149.0.7827.155 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	4.3	More Details
CVE-2026-12111	The Appointment Booking Calendar plugin for WordPress is vulnerable to Sensitive Information Exposure in versions up to, and including, 1.4.01. This is due to insufficient authorization and missing per-calendar ownership checks in the cpabc_appointments_calendar_load2() function, which is reachable via the cpabc_calendar_load2=1 query parameter in wp-admin and only checks is_admin() && current_user_can('edit_posts'), a capability available to Contributor-level users and above. This makes it possible for authenticated attackers with Contributor-level access and above to supply an arbitrary calendar ID via the id parameter and extract customer booking information, including email addresses, names, phone numbers, booking times, and comments, from any calendar managed by the plugin.	4.3	More Details
CVE-2026-35162	Dell PowerFlex Manager, version(s) [Versions], contain(s) an Improper Access Control vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to denial of service.	4.3	More Details
CVE-2026-49288	Statamic is a Laravel and Git powered content management system (CMS). Prior to 5.73.23 and 6.20.0, an authenticated Control Panel user could view metadata and content for resources they don't have permission to view, including entries, assets, users, roles, groups, and other configured resources. Depending on the resource, this could expose titles, custom field values, entry content, asset metadata, and the existence of users, roles, and groups. No data could be modified. This has been fixed in 5.73.23 and 6.20.0.	4.3	More Details
CVE-2026-24610	Subscriber Broken Access Control in MetForm Pro <= 3.9.1 versions.	4.3	More Details
CVE-2026-56384	Craft CMS contains a missing authorization vulnerability in the assets/preview-thumb endpoint. A Control Panel user without permission to view a target private asset can call the endpoint with an attacker-controlled assetId and receive preview HTML containing a signed fallback transform preview link for that private asset, because no asset-view permission check is performed before preview generation. This affects versions >= 4.0.0-RC1, <= 4.17.7 and >= 5.0.0-RC1, <= 5.9.13, and is fixed in 4.17.8 and 5.9.14.	4.3	More Details
CVE-2026-56385	Craft CMS versions >= 5.0.0-RC1, <= 5.9.13 and >= 4.0.0-RC1, <= 4.17.7 contain an authorization bypass in the assets/preview-file endpoint. The action does not enforce per-asset view authorization before returning preview content, allowing an authenticated low-privileged user to supply a controlled assetId for an asset they are not permitted to view and still receive preview response data (previewHtml), including a private preview image route containing the target private assetId. Fixed in 5.9.14 and 4.17.8.	4.3	More Details
CVE-2026-52846	Caddy is an extensible server platform that uses TLS by default. Prior to 2.11.4, Caddy’s stripHTML template function cannot reliably remove all HTML tags from input strings. Certain malformed HTML, such as <<>img src=x onerror=alert()>, can bypass the tag-stripping logic, potentially leaving dangerous content in the output if it is later rendered as HTML. This may allow client-side XSS in cases where untrusted strings are rendered unsafely. This vulnerability is fixed in 2.11.4.	4.2	More Details
CVE-2026-12457	Inappropriate implementation in Extensions in Google Chrome prior to 149.0.7827.155 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. (Chromium security severity: High)	4.2	More Details
	Daytona is a secure and elastic infrastructure runtime for AI-generated code execution and		

CVE-2026-54319	agent workflows. Prior to 0.186, a sandbox volume reference (volumeId, which may also be a volume name) was forwarded to the runner and used to build the host bind-mount source path without confinement. A reference containing path-traversal sequences could in principle resolve the mount source outside the intended per-volume base directory. This vulnerability is fixed in 0.186.	4.2	More Details
CVE-2026-12460	Insufficient policy enforcement in File System Access in Google Chrome prior to 149.0.7827.155 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted PDF file. (Chromium security severity: High)	4.2	More Details
CVE-2026-12456	Inappropriate implementation in Extensions in Google Chrome prior to 149.0.7827.155 allowed an attacker who convinced a user to install a malicious extension to bypass same origin policy via a crafted Chrome Extension. (Chromium security severity: High)	4.2	More Details
CVE-2026-48776	LangGraph Python SDK is used to connect to running LangGraph API servers, manage assistants, threads and stream runs from Python applications. Versions 0.3.14 and prior have unsafe URL path construction through unsanitized caller-supplied identifier values used in HTTP request paths for resource operations. Without sanitization of those values, identifiers that contain characters with special meaning in URL paths could cause the resulting request to address a different resource (and potentially a different resource type) than the SDK method's call site indicates. In deployments where the SDK receives identifier values that originate from untrusted sources, this could result in unintended access, modification, or deletion of resources beyond the calling user's authorization scope. This issue is most consequential in deployments that forward end-user-supplied values directly into SDK identifier parameters without first validating them against an expected format (such as a UUID), and rely on URL-prefix-based authorization at an upstream layer (reverse proxy, edge gateway, WAF), where the authorization decision is made on the SDK call's intended path rather than on the final delivered request path. The issue has been fixed in version 0.3.15.	4.2	More Details
CVE-2026-54298	Astro is a web framework. Prior to 6.4.6, the spreadAttributes function in Astro's server-side rendering pipeline iterates over object keys and passes them directly to addAttribute, which interpolates the key into the HTML output without escaping. When a developer uses the spread syntax {...props} on an HTML element and the object keys come from an untrusted source (API, CMS, URL parameters), an attacker can inject arbitrary HTML attributes including event handlers like onmousemove, onclick, or break out of the attribute context entirely to inject new elements. This vulnerability is fixed in 6.4.6.	4.2	More Details
CVE-2026-12453	Insufficient validation of untrusted input in Input in Google Chrome prior to 149.0.7827.155 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page. (Chromium security severity: High)	4.2	More Details
CVE-2026-46771	Vulnerability in the Oracle Application Development Framework (ADF) product of Oracle Fusion Middleware (component: Java Business Objects). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Application Development Framework (ADF) executes to compromise Oracle Application Development Framework (ADF). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Application Development Framework (ADF) accessible data. CVSS 3.1 Base Score 4.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N).	4.1	More Details
CVE-2026-4983	Open VSX Registry does not sanitize SVG files uploaded as extension icons prior to storage, and serves them with Content-Type: image/svg+xml without security headers such as Content-Security-Policy or Content-Disposition: attachment. This allows an attacker to publish an extension with a malicious SVG icon and achieve stored cross-site scripting (XSS) when a user navigates directly to the icon URL. On deployments using local storage, script execution occurs within the Open VSX application origin, enabling session hijacking, authentication token theft, and unauthorized extension publishing. On deployments backed by external storage (such as open-vsx.org with an S3-backed CDN), execution is confined to the storage origin, reducing impact but still permitting phishing attacks and credential harvesting through attacker-crafted pages.	4.1	More Details
CVE-2026-57053	GNU libidn before 1.44 is prone to out-of-bounds reads of uninitialized memory in the ToUnicode APIs because of mishandling in idna_to_unicode_internal. The affected code is not present in libidn2.	4.0	More Details

CVE-2026-56357	n8n before 1.123.15 and 2.5.0 contains a webhook forgery vulnerability in the GitHub Webhook Trigger node that fails to implement HMAC-SHA256 signature verification. Attackers who know the webhook URL can send unsigned POST requests to trigger workflows with arbitrary data, spoofing GitHub webhook events.	4.0	More Details
CVE-2026-8823	Mattermost versions 11.7.x <= 11.7.0, 10.11.x <= 10.11.17 fail to validate bot targets when demoting users to guests which allows a lower-privileged administrator to degrade arbitrary bot accounts via the standard demote-user API.. Mattermost Advisory ID: MMSA-2026-00669	3.8	More Details
CVE-2026-56212	Capgo before 12.128.2 contains an authentication logic flaw: a user with permission to manage team or organization security settings can enable mandatory two-factor authentication for all team members without first enabling 2FA on their own account. The application fails to verify the initiator's 2FA status before allowing the policy change, resulting in inconsistent security enforcement, potential administrative misuse, and lockout risk for team members.	3.8	More Details
CVE-2026-8074	Mattermost versions 11.7.x <= 11.7.0, 10.11.x <= 10.11.17 fail to enforce bot-specific permission checks on the user active status endpoint, which allows a User Manager with user management write access but no Integrations access to deactivate bot accounts via the PUT /api/v4/users/{id}/active API endpoint.. Mattermost Advisory ID: MMSA-2026-00667	3.8	More Details
CVE-2026-56376	ImageMagick before 7.1.2-15 and 6.9.13-40 contains a heap use-after-free in the meta coder: when memory allocation fails, a single byte is written to a stale pointer. Remote attackers can trigger it by processing specially crafted image files, causing a denial of service.	3.7	More Details
CVE-2026-56968	GNU SASL before 2.2.4 lacks sanitization of a short challenge in _gsasl_ntlm_client_step in the NTLM client, which could result in memory disclosure via a crafted server.	3.7	More Details
CVE-2026-56367	ImageMagick before 7.1.2-15 and 6.9.x before 6.9.13-40 contains an integer overflow in the PSB (PSD v2) RLE decoding path (ReadPSDChannelRLE in coders/psd.c) that causes a heap out-of-bounds read on 32-bit builds. Processing a crafted PSB file can lead to information disclosure or a crash.	3.7	More Details
CVE-2026-11525	Impact: When undici parses a Set-Cookie header, it accepts any SameSite attribute value that contains Strict, Lax, or None as a substring, rather than the case-insensitive exact match specified by RFC 6265. Non-spec values are silently mapped to one of the three standard tokens. For example, SameSite=NoneOfYourBusiness is parsed as None (the most permissive setting), and SameSite=StrictLax is parsed as Lax (a downgrade from Strict). Affected applications are those that consume Set-Cookie headers from server responses (for example via undici's fetch or proxy code paths) and then forward or rely on the parsed sameSite attribute. A malicious or non-compliant server can coerce the consumer's view of a cookie's SameSite policy to a weaker value, silently degrading the SameSite enforcement the cookie is supposed to provide. This was introduced in undici 5.15.0 when the cookies feature was added. Patches: Upgrade to undici v6.26.0, v7.28.0 or v8.5.0. Workarounds: After parsing a Set-Cookie header, validate that the resulting sameSite attribute is one of 'Strict', 'Lax', or 'None' (exact, case-insensitive) before forwarding or relying on it.	3.7	More Details
CVE-2026-53540	Python-Multipart is a streaming multipart parser for Python. Prior to 0.0.31, parse_form() did not validate the Content-Length header before using it to bound its chunked read of the request body. A negative Content-Length turned the bounded read into a read-until-EOF, so the entire body was loaded into memory in a single read instead of in fixed-size chunks. This vulnerability is fixed in 0.0.31.	3.7	More Details
CVE-2026-9143	There is an incorrect conversion between numeric types vulnerability in NI grpc-device due to missing range checks in CodeGen. This may silently discard high bits if a size value exceeded the target type's range. This affects NI grpc-device 2.17.0 and prior versions.	3.7	More Details
CVE-2026-54282	Starlette is a lightweight ASGI framework/toolkit. Prior to 1.3.0, the HTTP request path is not validated before being used to reconstruct request.url. Because request.url is rebuilt by concatenating {scheme}://{host}{path} and re-parsing the result, a path that does not begin with / (for example @google.com) moves the authority boundary during re-parsing, so request.url.hostname and request.url.netloc become attacker-controlled. Code that reads request.url.hostname (rather than the Host header or scope) can therefore be misled into trusting an attacker-supplied host. This vulnerability is fixed in 1.3.0.	3.7	More Details
CVE-			More

2026-56355	GNU Savannah Administration Savane through 3.17 uses untrusted data as part of authorization.	3.7	Details
CVE-2026-53538	Python-Multipart is a streaming multipart parser for Python. Prior to 0.0.30, QuerystringParser treated ; as a field separator in application/x-www-form-urlencoded bodies, in addition to &. The WHATWG URL standard, modern browsers, and Python's urllib.parse (since the CVE-2021-23336 fix) treat only & as a separator. This creates a parser differential: the same bytes are tokenized into different fields than a WHATWG compliant intermediary would produce, allowing an attacker to smuggle extra form fields past an upstream body inspecting component. This vulnerability is fixed in 0.0.30.	3.7	More Details
CVE-2026-55654	A flaw was found in OpenSSH. This vulnerability, a heap out-of-bounds read, occurs during the cleanup of GSSAPI (Generic Security Service Application Programming Interface) indicators when a trailing NULL termination is missing in the auth-indicators array. A remote attacker, under specific configurations involving GSSAPI authentication and a Kerberos environment, could exploit this to cause the SSH authentication path to crash or abort. This leads to a denial of service (DoS), impacting the availability of the SSH service.	3.7	More Details
CVE-2026-6733	Impact: Undici's HTTP/1.1 client is vulnerable to response queue poisoning on reused keep-alive sockets. An attacker-controlled upstream server can inject an unsolicited HTTP/1.1 response onto an idle socket after a request completes. When the client dispatches the next request on that socket, it associates the injected response with the new request, causing responses to be delivered to the wrong requests. This requires an attacker-controlled or compromised upstream HTTP/1.1 server and keep-alive connection reuse. Patches: Upgrade to undici v6.26.0, v7.28.0 or v8.5.0. Workarounds: Disable keep-alive connection reuse by setting keepAliveTimeout: 0 on the Client or Pool.	3.7	More Details
CVE-2026-53537	Python-Multipart is a streaming multipart parser for Python. Prior to 0.0.30, parse_options_header parsed Content-Disposition (and Content-Type) headers with email.message.Message, which transparently applies RFC 2231/5987 decoding. The extended parameter syntax (filename*=charset'lang'value, name*=..., and the filename*0/filename*1 continuation form) is decoded and surfaced under the bare filename/name key, and overrides the plain parameter when both are present. RFC 7578 §4.2 explicitly forbids the filename* form in multipart/form-data. Components that follow RFC 7578, or that do not implement RFC 2231/5987 decoding for multipart/form-data (WAFs, proxies, gateways), may interpret such a header differently. An attacker can exploit that difference to smuggle a different field name or filename past an upstream inspector to the backend. This vulnerability is fixed in 0.0.30.	3.7	More Details
CVE-2026-56378	ImageMagick before 7.1.2-15 (and 6.x before 6.9.13-40) contains a heap out-of-bounds read in the PCD coder's DecodeImage loop. A crafted PCD file can trigger a one-byte heap out-of-bounds read during image decoding, resulting in denial of service and potential disclosure of an adjacent heap byte.	3.7	More Details
CVE-2026-12047	HTML injection in pgAdmin 4's cloud deployment module. The verify_credentials, deploy, regions, and update-server endpoints under /rds/, /azure/, /google/, and the top-level /cloud/ blueprint propagated AWS / Azure / Google SDK exception text — and the related file-resolution and database-commit exception text — into the JSON response body (the info and errormsg fields) without HTML-encoding. The Cloud Wizard frontend rendered these strings through html-react-parser, so an attacker-influenced exception message embedded structural HTML directly into the wizard's DOM. The reported entry point is /rds/verify_credentials/. An authenticated pgAdmin user submits a crafted access_key whose value contains an <iframe/src=...> payload; AWS STS rejects the credential with an IncompleteSignature exception whose text quotes the access_key verbatim; the pgAdmin backend forwards that text into the JSON info field; the Cloud Wizard's FormFooterMessage parses it as HTML. The browser fetches the iframe's src from an attacker-controlled host, and JavaScript executing inside the cross-origin iframe writes to parent.location, redirecting the victim's pgAdmin tab. Because the injection renders inside pgAdmin's own interface, X-Frame-Options and Content-Security-Policy frame-ancestors do not mitigate it. Baseline impact is self-targeted (the same user who supplied the payload sees the injection); escalation against other authenticated users requires an additional cross-site request-forgery primitive capable of submitting the malformed credential request with a valid X-pgA-CSRFToken in the victim's browser context. The same unsanitised-error-into-JSON pattern was present across multiple sibling endpoints — Azure's check_cluster_name_availability, every Google endpoint that surfaces SDK errors (verification_ack, projects, regions, instance_types, database_versions, the verify_credentials path-resolution branches), the central /deploy endpoint that bubbles str(e) from deploy_on_rds / deploy_on_azure / deploy_on_google, and	3.5	More Details

	update_cloud_server which surfaces the str(e) from a failing db.session.commit — all of which are now covered. Fix HTML-escapes every external/SDK exception string at the endpoint sink via a new shared sanitize_external_text helper (HTML escape with control-character strip), promoted out of the psycopg3 driver into web/pgadmin/utils/text_sanitize.py. The Cloud Wizard frontend additionally renders its FormFooterMessage in plain-text mode for backend-derived strings, so the value is never parsed as HTML even if a future sink forgets the escape. This issue affects pgAdmin 4: from 6.6 before 9.16.		
CVE-2026-56330	Capgo before 12.128.2 contains an open redirect vulnerability in stripe_portal and stripe_checkout endpoints that accept unvalidated callbackUrl, successUrl, and cancelUrl parameters. Authenticated attackers can craft malicious billing URLs to redirect users to attacker-controlled domains for phishing and credential harvesting.	3.5	More Details
CVE-2025-15619	HCL Connections contains a broken access control vulnerability that may allow an unauthorized user to view data in a single specific scenario.	3.5	More Details
CVE-2026-35068	Dell PowerFlex Manager, version(s) [Versions], contain(s) an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability. A low privileged attacker with adjacent network access could potentially exploit this vulnerability, leading to information disclosure.	3.5	More Details
CVE-2026-12812	A security vulnerability has been detected in Radware Cyber Controller up to 10.11.0. This affects an unknown part of the component HTML Report Generation. The manipulation leads to HTML injection. Remote exploitation of the attack is possible. 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.	3.5	More Details
CVE-2026-0057	In Contacts Provider, there is a possible way to access an incoming call's phone number and associated metadata due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	3.3	More Details
CVE-2026-12823	A security flaw has been discovered in Browserbase up to 20260526. This impacts an unknown function of the component Autobrowse Trace Artifact Handler. The manipulation results in incorrect default permissions. The attack requires a local approach. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	3.3	More Details
CVE-2026-46977	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: VMSVGA device). The supported version that is affected is 7.2.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 3.2 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:N).	3.2	More Details
CVE-2026-49356	Babel is a compiler for writing next generation JavaScript. Prior to 8.0.0-rc.6 and 7.29.6, @babel/core affected by an arbitrary file read via a sourceMappingURL comment. Using @babel/core to compile maliciously crafted code can allow an attacker to read any source map from the system that is running Babel, if the attacker controls the input source code, can read the output source code, and knows the path of the source map file that they want to read. This vulnerability is fixed in 8.0.0-rc.6 and 7.29.6.	3.2	More Details
CVE-2026-46815	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: VMSVGA device). The supported version that is affected is 7.2.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 3.2 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:N).	3.2	More Details
	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: VMSVGA		

CVE-2026-46816	device). The supported version that is affected is 7.2.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 3.2 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:N).	3.2	More Details
CVE-2026-46874	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.2.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 3.2 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:N).	3.2	More Details
CVE-2025-62340	HCL iControl was affected by Inadequate Session Timeout vulnerability. The vulnerability involves a security risk where a web application fails to automatically terminate user sessions after a period of inactivity	3.1	More Details
CVE-2026-12458	Inappropriate implementation in Passwords in Google Chrome prior to 149.0.7827.155 allowed a remote attacker who convinced a user to engage in specific UI gestures to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	3.1	More Details
CVE-2026-53663	React Router is a router for React. From 7.12.0 until 7.15.1, certain CSRF checks in React Router v7 Framework Mode were insufficient and run on POST requests, but were bypassed on PUT/PATCH/DELETE requests. This is a low severity vulnerability because modern browser protections (CORS preflight, SameSite cookies) already block the cross-origin attack vectors that this missing CSRF check would otherwise gate. This vulnerability is fixed in 7.15.1.	3.1	More Details
CVE-2026-12566	The docker_pull module uses the realm parameter from a Docker registry's WWW-Authenticate response header as the authentication endpoint without validation. An attacker in a man-in-the-middle position between bbot and a Docker registry could modify this header to redirect the authentication request to an arbitrary endpoint, potentially leaking authentication tokens.	3.1	More Details
CVE-2026-56325	Capgo before 12.128.2 uses ILIKE pattern matching instead of exact matching for app_id lookup in the preview subdomain resolver, allowing underscore characters in app_id to act as SQL wildcards. Attackers can create apps with app_ids differing by one character at underscore positions to cause unintended pattern matches, breaking preview functionality for legitimate apps or causing app-id confusion.	3.1	More Details
CVE-2026-49358	PhpWeasyPrint is a PHP library allowing PDF generation from a URL or an HTML page. Prior to version 2.6.0, `AbstractGenerator::$temporaryFiles` is a public array, and `removeTemporaryFiles()` — invoked from `__destruct()` and from a registered shutdown function — calls `unlink()` on every entry without verifying that the path is contained within the temporary folder. Any code holding a reference to a generator instance can push an arbitrary path into the array and have it deleted on script shutdown. This mirrors the KnpLabs/snappy issue GHSA-87qc-37cw-84h4. PhpWeasyPrint version 2.6.0 contains a patch for the issue.	3.0	More Details
CVE-2026-39199	snes9x 1.63 allows an out-of-bounds write and denial of service via a crafted .ups file.	2.9	More Details
CVE-2026-57062	CMS (Cryptographic Message Syntax) parsing in gpgsm in GnuPG through 2.5.20 mishandles the CMS format for AES-GCM because aes-ICVlen is supposed to be 12 bytes but 4 bytes is accepted. NOTE: this is related to CVE-2026-34182.	2.9	More Details
CVE-2026-12102	The UsersWP – Front-end login form, User Registration, User Profile & Members Directory plugin for WP plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 1.2.63 via the 'user_id' parameter due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with editor-level access and above, to reset and permanently delete the avatar or banner image of any arbitrary user, including administrators, by clearing their avatar_thumb or banner_thumb metadata in the uwp_usermeta table.	2.7	More Details

CVE-2026-54326	Pi is a minimal terminal coding harness. From 0.74.0 until 0.78.1, Pi HTML exports render session Markdown into a static HTML file. It did not consistently reject unsafe Markdown link and image URL schemes. In versions with scheme filtering, C0 control characters in the URL scheme could bypass the check because browsers normalize those characters before navigation. This vulnerability is fixed in 0.78.1.	2.5	More Details
CVE-2026-9610	IBM Datacap 9.1.7, 9.1.8, and 9.1.9 and IBM Datacap Navigator 9.1.7, 9.1.8, and 9.1.9 exposes resources or functionality that isn't linked in the UI but is accessible by directly requesting the URL, bypassing intended access controls.	2.3	More Details
CVE-2026-12567	The github_workflows module constructs local directory paths from user-controlled repository names without validating for symlinks. A local attacker sharing the scan directory can plant a symlink at the predictable output path, causing workflow data to be written to an attacker-chosen location.	2.2	More Details
CVE-2026-54327	Pi is a minimal terminal coding harness. From 0.74.0 until 0.78.1, Pi stored API keys and OAuth credentials in auth.json. A race condition in the file write path could briefly create or rewrite this file with permissions derived from the process umask before tightening the file to owner-only permissions. This vulnerability is fixed in 0.78.1.	2.2	More Details
CVE-2026-46549	NocoDB is software for building databases as spreadsheets. Prior to 2026.04.1, the OAuth token strategy attached oauth_scope and oauth_granted_resources to the request user, but the ACL middleware never consulted either. An OAuth token issued with a restricted scope (e.g. MCP-only) therefore inherited the full permissions of the underlying user across all routes; the granted_resources.base_id restriction was bypassed on org-level endpoints that don't populate req.context.base_id. This vulnerability is fixed in 2026.04.1.	2.0	More Details
CVE-2026-50268	Steeltoe is an open source project that provides a collection of libraries that helps users build cloud-native applications. In Steeltoe.Configuration.Encryption 4.0.0 through 4.1.0, configuring `encrypt:rsa:algorithm=OAEP` does not enable OAEP encryption. Due to an incorrect BouncyCastle transformation string, the `OAEP` setting selects PKCS#1 v1.5, which is the same algorithm as the `DEFAULT` setting. Steeltoe.Configuration.Encryption version 4.2.0 patches the issue.	1.9	More Details
CVE-2026-56371	ImageMagick before 7.1.2-15 and 6.9.13-40 contains a memory leak in coders/txt.c when processing TXT files with texture attributes: the texture object allocated via ReadImage is not released when GetTypeMetrics fails, leaking memory each time a crafted TXT file with a texture attribute is processed.	0.0	More Details
CVE-2026-56379	ImageMagick before 7.1.2-15 and 6.9.13-40 contains a command injection vulnerability in the SVG decoder that allows attackers to inject arbitrary MVG drawing commands. Attackers can craft malicious SVG files with injected Magick Vector Graphics commands that execute during rendering.	0.0	More Details
CVE-2026-47378	NocoDB is software for building databases as spreadsheets. Prior to 2026.04.1, Public shared-view endpoints exposed values from columns that the view owner had hidden, via three independent paths: groupBy returned raw values for any column named in the request, filter and sort arrays operated on hidden columns enabling boolean-blind extraction, and the related-data list accepted arbitrary link-column IDs from other tables in the same base. This vulnerability is fixed in 2026.04.1.	N/A	More Details
CVE-2026-12039	Docker Sandboxes (sbx) enforces an HTTP/S-only egress allowlist but does not apply it to DNS resolution: the per-network embedded DNS server forwards any queried name to the host resolver whenever the network is internet-connected, without consulting the policy. A workload inside a sandbox, which the threat model treats as untrusted, can therefore encode data into DNS labels for an attacker-controlled domain and exfiltrate it through a DNS covert channel, bypassing the configured allowlist.	N/A	More Details
CVE-2025-64105	FOSSBilling is a billing and client management system that automates invoicing, payments, and communication for online service businesses. Versions 0.6.21 through 0.7.2 are vulnerable to IDOR through the support ticket creation workflow. By manipulating rel_id when rel_type=order, an authenticated client can create a support ticket that references another client's order they do not own. The ticketCreateForClient() method accepted rel_id without verifying order ownership for non-upgrade tasks, allowing clients to link a new ticket to another client's order by crafting the request. No cron task automatically processes cancel/upgrade requests from ticket relations;	N/A	More Details

	staff action is required. This affects integrity and confidentiality: staff could be misled into acting on the wrong order (e.g., cancellation or upgrade requests). While there is no client-to-client order data exposure, order IDs may appear in ticket context. This issue has been fixed in version 0.8.0.		
CVE-2026-49465	n8n is an open source workflow automation platform. Prior to 1.123.48, 2.21.8, and 2.22.4, an authenticated user with permission to create or modify workflows could supply a local filesystem path as the source repository in the Git node's Clone operation, or as the target repository in the Push operation, bypassing the N8N_RESTRICT_FILE_ACCESS_TO file sandbox. This allowed the contents of any local git repository accessible to the n8n process to be cloned into an allowed path and read, circumventing the access restrictions that correctly blocked direct file reads to the same paths. This vulnerability is fixed in 1.123.48, 2.21.8, and 2.22.4.	N/A	More Details
CVE-2026-54762	Traefik is an HTTP reverse proxy and load balancer. From 3.7.0-ea.1 until 3.7.5, there is a medium severity vulnerability in Traefik's Kubernetes Ingress NGINX provider that causes affected routes to fail open. When an Ingress explicitly enables BasicAuth or DigestAuth through the supported nginx.ingress.kubernetes.io/auth-type and auth-secret annotations, but the referenced auth Secret cannot be resolved or parsed, Traefik logs the resolution error, skips installing the authentication middleware, and still emits a router to the backend service. A route that operators intended to protect is therefore published to the data plane without its authentication control, allowing unauthenticated access to the backend. The trigger is an invalid or unresolved auth dependency — a missing, malformed, unreadable, or policy-denied Secret — rather than an intentionally unprotected route. This vulnerability is fixed in 3.7.5.	N/A	More Details
CVE-2026-54761	Traefik is an HTTP reverse proxy and load balancer. Prior to 3.6.21 and 3.7.5, there is a high severity vulnerability in Traefik's Kubernetes Gateway provider affecting the crossProviderNamespaces allowlist. For HTTPRoute rules that declare multiple (WRR) backendRefs, Traefik evaluates the allowlist against the target backendRef.namespace instead of the route's own namespace. As a result, an HTTPRoute created in a namespace that is not allow-listed can reference a cross-provider TraefikService such as api@internal, dashboard@internal or rest@internal by pointing backendRef.namespace at an allow-listed namespace covered by a Gateway API ReferenceGrant, exposing internal Traefik services on the data plane. Exploitation requires the ability to create an accepted HTTPRoute and a matching ReferenceGrant from an allow-listed namespace; it does not require any change to Traefik static configuration, RBAC, or the deployment itself. This vulnerability is fixed in 3.6.21 and 3.7.5.	N/A	More Details
CVE-2026-2675	Missing Authentication for Critical Function vulnerability in RTI Connext Professional (Security Plugins) allows Fake the Source of Data.This issue affects Connext Professional: from 7.4.0 before 7.7.0, from 7.0.0 before 7.3.1.3, from 6.1.0 before 6.1.*, from 6.0.0 before 6.0.*, from 5.3.0 before 5.3.*.	N/A	More Details
CVE-2026-56120	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority as it's a duplicate of CVE-2026-56784.	N/A	More Details
CVE-2026-12527	A broken authorization boundary in the RTSP media delivery pipeline of Shenzhen Liandian Communication Technology LTD V380 IP Camera firmware AppFHE1_V1.0.6.020230803 enables unauthenticated network actors to bypass the device’s credential-enforced live-view workflow and directly retrieve real-time video stream data.	N/A	More Details
CVE-2026-54301	n8n is an open source workflow automation platform. Prior to 1.123.55, 2.25.7, and 2.26.2, an authenticated user with workflow edit access could configure a Respond to Webhook node to serve binary content with an attacker-controlled Content-Type. The binary response path bypassed the central Content-Security-Policy sandbox header, allowing a public webhook to execute JavaScript in the n8n origin when visited by an authenticated user, with access to that user's session. This vulnerability is fixed in 1.123.55, 2.25.7, and 2.26.2.	N/A	More Details
CVE-2026-54302	n8n is an open source workflow automation platform. Prior to 1.123.55, 2.25.7, and 2.26.2, an authenticated user with workflow edit access could inject arbitrary JavaScript into the Chat Trigger's generated page by setting a malicious webhookId. When a logged-in user visited the chat URL, the injected code executed in the n8n origin with that user's session privileges. This vulnerability is fixed in 1.123.55, 2.25.7, and 2.26.2.	N/A	More Details
	Docker Sandboxes (sbx) blocks ICMP egress with an authorizer applied only at network-creation time, and does not re-apply it to networks rebuilt from disk when the Docker daemon restarts,		

CVE-2026-12539	so a restart-surviving sandbox forwards ICMP to arbitrary hosts. A workload inside a sandbox, which the threat model treats as untrusted, can therefore defeat the documented ICMP egress block to perform network reconnaissance and exfiltrate data over an ICMP covert channel, regardless of the configured allowlist.	N/A	More Details
CVE-2026-49290	Slopsmith is a self-contained web application for browsing, playing, and practicing Rocksmith 2014 Custom DLC (CDLC). Prior to 0.2.9-alpha.5, a path-traversal vulnerability in Slopsmith's archive extractors allows an attacker to write arbitrary files outside the extraction directory by supplying a crafted PSARC or sloppak archive. With the default Docker configuration (running as root) and the ability to drop a file into the plugin directory, this escalates to arbitrary remote code execution on the host. Three archive extractors concatenated archive-entry filenames directly onto the extraction root without validation: `lib/psarc.py::unpack_psarc` — PSARC TOC filenames; `lib/patcher.py::unpack_psarc` — duplicate of the above in the patcher flow; `lib/sloppak.py::_unpack_zip` — bare `ZipFile.extractall()` with no member filter. Each accepts entry names containing `..` segments, absolute paths, or backslash separators. The Python `zipfile` module's default `extractall()` is documented as not preventing traversal when callers don't supply a member-filter callback. Version 0.2.9-alpha.5 patches the issue. Until updated, do not open PSARC or sloppak archives from untrusted sources, and do not expose the Slopsmith instance to the public internet. Docker users should also pull the latest image after the next slopsmith Docker image is published.	N/A	More Details
CVE-2026-8811	SEPPmail versions before 15.0.5 allow improper handling of attachment filenames during encrypted PDF generation. An attacker can exploit this to create new files outside the intended directory, potentially placing files in web-accessible locations.	N/A	More Details
CVE-2026-54304	n8n is an open source workflow automation platform. Prior to 1.123.55, 2.25.7, and 2.26.1, an authenticated user with permission to create or modify workflows and access to a SecurityScorecard credential with limited allowed domains could configure the SecurityScorecard node's report download operation to target an attacker-controlled URL. The node attached the SecurityScorecard API token to the outbound request, causing the credential to be sent to the attacker-controlled host bypassing credential configured limitations and exfiltrating. This vulnerability is fixed in 1.123.55, 2.25.7, and 2.26.1.	N/A	More Details
CVE-2026-54305	n8n is an open source workflow automation platform. Prior to 1.123.55, 2.25.7, and 2.26.2, three EE endpoints used by the Dynamic Credentials feature accepted any authenticated n8n session without performing per-resource ownership or scope checks on the target workflow or credential. An authenticated user with no project membership or credential sharing relationship could enumerate credential identifiers, names, and types referenced by any private workflow in the instance, initiate an OAuth authorization flow against another user's credential to overwrite its stored tokens with tokens bound to an account they control, or revoke another user's stored credential tokens entirely. Workflows relying on a hijacked credential would subsequently execute under the attacker's OAuth identity, enabling data exfiltration to attacker-controlled external services and persistent takeover of integrations. Token revocation would break affected workflows. This vulnerability is fixed in 1.123.55, 2.25.7, and 2.26.2.	N/A	More Details
CVE-2026-54306	n8n is an open source workflow automation platform. Prior to 2.25.7 and 2.26.2, a prototype pollution vulnerability allowed a crafted public webhook payload to inject attacker-controlled fields into workflow data during internal object copying. These fields could be surfaced and consumed as normal values by downstream built-in nodes. Where a workflow combines a public webhook with action nodes that consume the resulting fields, an attacker could cause the workflow to act as a confused deputy — targeting unintended records or issuing outbound requests using the workflow owner's configured credentials. This vulnerability is fixed in 2.25.7 and 2.26.2.	N/A	More Details
CVE-2026-53622	Traefik is an HTTP reverse proxy and load balancer. Prior to 3.7.3, there is a critical vulnerability in Traefik's HTTP/3 (QUIC) TLS configuration selection that allows unauthenticated clients to bypass router-specific mTLS enforcement. When HTTP/3 is enabled on an entrypoint, the TLS handshake selects the applicable TLS configuration through an exact, case-sensitive lookup on the SNI value, which fails to match wildcard host patterns (e.g., *.example.com) or case variants of the configured hostname. Because the handshake falls back to the default TLS configuration — which may not require client certificates — a client can complete the QUIC handshake without presenting a certificate, while the subsequent HTTP routing layer still dispatches the request to a backend protected by a router-specific mTLS policy. The issue affects deployments where HTTP/3 is enabled, a router uses a wildcard Host rule or case-insensitive hostname matching, a router-specific TLSOptions enforces client certificate authentication, and UDP access to the	N/A	More Details

	entrypoint is reachable by an attacker. This vulnerability is fixed in 3.7.3.		
CVE-2026-54307	n8n is an open source workflow automation platform. Prior to 1.123.55, 2.25.7, and 2.26.2, a member-level user with editor access to a shared workflow could reference credentials they do not own via specific public API endpoints. Credential ownership checks were only enforced partially leading to cross-user credential access. This issue affects instances where workflow sharing is enabled and at least one workflow has been shared with a member-level user as an Editor. This vulnerability is fixed in 1.123.55, 2.25.7, and 2.26.2.	N/A	More Details
CVE-2026-48491	Traefik is an HTTP reverse proxy and load balancer. From 3.7.0 until 3.7.3, there is a high severity vulnerability in Traefik's domain-fronting protection (SNICheck) that allows an unauthenticated client to bypass mutual TLS enforced through wildcard router TLSOptions. When a router uses a wildcard host rule such as Host(*.example.com) with stricter TLS options (for example RequireAndVerifyClientCert), SNICheck resolves the TLS options for the HTTP Host header using exact map lookups only and never applies wildcard matching. If another permissive SNI is served on the same entrypoint, an attacker can complete the TLS handshake under the permissive options and then send an HTTP Host header targeting the wildcard-protected backend, reaching it without presenting a client certificate. This affects the regular HTTPS / HTTP-2 path and does not require HTTP/3. This vulnerability is fixed in 3.7.3.	N/A	More Details
CVE-2026-54308	n8n is an open source workflow automation platform. Prior to 2.25.7 and 2.26.2, the MicrosoftAgent365Trigger and StripeTrigger node did not validate that inbound requests. As a result, an unauthenticated attacker who knows the webhook URL could submit a forged payload and cause the workflow to execute with attacker-controlled data. This vulnerability is fixed in 2.25.7 and 2.26.2.	N/A	More Details
CVE-2026-2674	Out-of-bounds Write, Out-of-bounds Write, Out-of-bounds Write vulnerability in RTI Connext Professional (Queueing Service,Core Libraries,Persistence Service) allows Overflow Buffers, Overflow Buffers, Overflow Buffers.This issue affects Connext Professional: from 7.4.0 before 7.7.0, from 7.0.0 before 7.3.1.3, from 6.1.0 before 6.1.*.	N/A	More Details
CVE-2026-48020	Traefik is an HTTP reverse proxy and load balancer. Prior to 2.11.48, 3.6.19, and 3.7.3, there is a high severity vulnerability in Traefik's StripPrefix middleware that allows an unauthenticated attacker to bypass route-level authentication and authorization. When a public router matches on a PathPrefix rule and applies the StripPrefix middleware, a request path containing .. or its percent-encoded form %2e%2e can match the public route at routing time and then, after the prefix is stripped and the path is normalized, resolve to a path served by a separate, authenticated router. As a result, an attacker can reach protected backend paths — such as admin or internal configuration endpoints — without satisfying the authentication middleware attached to the protected router. This vulnerability is fixed in 2.11.48, 3.6.19, and 3.7.3.	N/A	More Details
CVE-2026-45792	rtk filters and compresses command outputs before they reach your LLM context. Prior to 0.32.0, RTK (Rust Token Killer) improperly trusts project-local configuration files. RTK automatically loads .rtk/filters.toml from the working directory with highest priority and without user notification. An attacker can place a malicious filter file in a repository to apply regex-based modifications (e.g., strip_lines_matching) to shell command output before it is shown to the LLM, without any indication that the output has been modified. This allows attackers to selectively suppress or alter command output (including file contents, diffs, and security scan results) without detection, potentially concealing malicious code during AI-assisted development or review. This vulnerability is fixed in 0.32.0.	N/A	More Details
CVE-2026-12845	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2026-11958	Local privilege escalation by loading DLLs from a shared temporary directory in ANSSI’s DFIR-ORC, versions 10.2.7 and prior. An attacker with prior access to the system, can place a malicious DLL in C:\Windows\Temp and wait for the application to be executed. Because DFIR-ORC is extracted and executed from that location with administrative privileges, the malicious library can be loaded automatically, allowing the attacker to gain administrator privileges on the affected machine.	N/A	More Details
CVE-2026-	n8n is an open source workflow automation platform. Prior to 1.123.48, 2.21.8, and 2.22.4, an authenticated user with permission to create or modify workflows containing a Python Code Node could escape the sandbox and achieve arbitrary code execution on the task runner	N/A	More Details

49444	container. This vulnerability is fixed in 1.123.48, 2.21.8, and 2.22.4.		
CVE-2026-46553	NocoDB is software for building databases as spreadsheets. Prior to 2026.04.1, the upload-by-URL path did not enforce NC_ATTACHMENT_FIELD_SIZE against either the remote file's advertised Content-Length or the decoded length of a data: URI, allowing an authenticated user to bypass the configured per-file size limit. This vulnerability is fixed in 2026.04.1.	N/A	More Details
CVE-2026-34917	Low-privileged session IDs generated for the web admin console could be reused in the XML-RPC API, whose authentication is normally restricted to admin users. An attacker could leverage this to gain unauthorised access and exploit API-level vulnerabilities. The session context (web/API) is now recorded along with other session data, preventing session IDs from being used interchangeably.	N/A	More Details
CVE-2026-11748	A vulnerability has been identified in centraldogma-server-auth-shiro versions prior to 0.84.0, where the SearchFirstActiveDirectoryRealm substitutes the login username into an LDAP search filter without neutralizing LDAP filter metacharacters, allowing an unauthenticated attacker to manipulate the filter to cause authentication confusion and enumerate the directory structure.	N/A	More Details
CVE-2026-11746	A vulnerability has been identified in centraldogma-server versions prior to 0.84.0, where enabling ZooKeeper replication without setting replication.secret causes the server to silently fall back to a hard-coded, publicly known secret. This default credential authenticates the embedded ZooKeeper ensemble, allowing an attacker with network access to read the full replication log or join the quorum and execute arbitrary replicated commands across the cluster.	N/A	More Details
CVE-2026-34912	A missing access control check when linking banners or campaigns to a zone through the zone-include.php script of Revive Adserver 6.0.6 and earlier, or via its API allows a low-privileged user could link their zones to banners or campaigns owned by other managers on the same instance, resulting in inconsistent ownership relationships. Ownership validation has been added to ensure that banners and campaigns can only be linked to zones managed by the same account.	N/A	More Details
CVE-2026-34913	A missing access control check when linking trackers to campaigns through the campaign-trackers.php script of Revive Adserver 6.0.6 and earlier could allow a low-privileged user to link their trackers to campaigns owned by other managers on the same instance, resulting in inconsistent ownership relationships. Ownership validation has been added to ensure that campaigns can only be linked to trackers owned by the same advertiser.	N/A	More Details
CVE-2026-34914	A missing sanitisation of user input in the zone-include.php script of Revive Adserver 6.0.6 and earlier. A low-privileged user could exploit the clientid parameter to perform blind SQL injection attacks. Input sanitisation has been improved to ensure that all parameters processed by the script are properly validated.	N/A	More Details
CVE-2026-11717	An authentication bypass vulnerability exists in the generic opaque token validation path (validateOpaqueToken) of googleapis/mcp-toolbox. When verifying an unparsed opaque token via an OAuth 2.0 introspection endpoint (RFC 7662), the toolbox decodes the response into an introspectResp struct where the Active field is declared as a pointer to a boolean (*bool). The code only explicitly rejects a token if the response contains a populated active field set to false (if introspectResp.Active != nil && !*introspectResp.Active). If an introspection endpoint responds with a payload that completely omits the mandatory active key, the internal variable remains nil, causing the conditional check to short-circuit. As a result, Toolbox accepts authorization tokens missing the "active" field, granting access to protected tools and underlying data sources.	N/A	More Details
CVE-2026-34915	A missing sanitisation of user input in the zone-include.php script of Revive Adserver 6.0.6 and earlier could allow a low-privileged user to exploit the clientid parameter to perform blind SQL injection attacks. Input sanitisation has been improved to ensure that all parameters processed by the script are properly validated.	N/A	More Details
CVE-2026-11718	An authentication bypass vulnerability exists in the generic opaque token validation path (validateOpaqueToken) of googleapis/mcp-toolbox. When the toolbox validates an opaque token via an OAuth 2.0 introspection endpoint (RFC 7662), it decodes the response into an introspectResp struct. However, the subsequent claim-checking logic (validateClaims) evaluates the issuer condition as if a.issuer != "" && iss != "". If the external OAuth provider's introspection response omits the optional iss (issuer) field completely, the variable iss defaults to an empty string. This causes the conditional block to evaluate to false and be skipped silently. Consequently, the application accepts tokens issued by unauthorized or unintended third-party	N/A	More Details

	identity providers.		
CVE-2026-56267	Flowise before 3.0.13 contains an information exposure vulnerability in the POST /api/v1/account/forgot-password endpoint that returns full user objects including PII to unauthenticated attackers. An attacker can enumerate valid email addresses and harvest sensitive user data including user IDs, names, account status, and timestamps by sending requests with known email addresses.	N/A	More Details
CVE-2026-11719	An authenticated authorization bypass vulnerability exists in MCP Toolbox for Databases due to missing scope enforcement across older protocol handlers. While the 2025-11-25 protocol version handler correctly enforces per-tool restrictions defined by scopesRequired, older supported protocol versions (2025-06-18, 2025-03-26, and 2024-11-05) omit this check. An authenticated client with low-privilege tokens (e.g., read) can bypass the intended per-tool scope restrictions and execute high-privilege tools (e.g., admin) simply by specifying an older protocol version in the MCP-Protocol-Version header, or by omitting the header entirely (which causes the server to default to the vulnerable 2024-11-05 handler).	N/A	More Details
CVE-2026-23513	FOSSBilling is a free, open-source billing and client management system. In versions 0.7.2 and prior, a query-construction flaw in client list endpoints allowed authenticated clients to bypass tenant scoping and retrieve other clients' data. Details In ServiceTransaction::getSearchQuery() and Order\Service::getSearchQuery(), OR-based search/action filters were appended without grouping, allowing SQL operator precedence to evaluate OR clauses independently of the enforced client_id constraint. Crafted requests could therefore return records and metadata belonging to other clients, including identifiers, amounts, status, timestamps, and related fields. This issue was fixed in version 0.8.0.	N/A	More Details
CVE-2026-34916	A missing validation of user input when saving delivery limitations in Revive Adserver 6.0.6 and earlier could allow a low-privileged user to use the logical parameter to inject malicious PHP code into the compiledlimitations field on the database and have it executed during banner delivery. Input sanitisation has been improved to ensure that the parameter is properly validated.	N/A	More Details
CVE-2026-56276	Flowise before 3.1.2 contains a mass assignment vulnerability in the PUT /api/v1/user endpoint that allows authenticated users to directly modify the credential field without validation. Attackers can bypass password change verification and session invalidation by supplying a crafted password hash, establishing persistent account access after temporary session compromise.	N/A	More Details
CVE-2026-11745	A vulnerability has been identified in centraldogma-server-mirror-git versions prior to 0.84.0, where the Git mirror SSH client does not verify remote host keys for git+ssh:// connections, allowing an on-path attacker to perform man-in-the-middle attacks and compromise mirrored repositories.	N/A	More Details
CVE-2026-11972	When using the "tarfile" module with a file opened in "streaming mode" (mode="r|") the tarfile module did not properly handle EOF, meaning an archive could be parsed in an infinite loop.	N/A	More Details
CVE-2026-44789	n8n is an open source workflow automation platform. Prior to 1.123.43, 2.22.1, and 2.20.7, an authenticated user with permission to create or modify workflows could achieve global prototype pollution via an unvalidated pagination parameter in the HTTP Request node. Combined with other techniques this could lead to RCE on the instance. This vulnerability is fixed in 1.123.43, 2.22.1, and 2.20.7.	N/A	More Details
CVE-2026-44790	n8n is an open source workflow automation platform. Prior to 1.123.43, 2.22.1, and 2.20.7, an authenticated user with permission to create or modify workflows could inject CLI flags on the Git node's Push operation allowing an attacker to read arbitrary files from the n8n server potentially leading to full compromise. This vulnerability is fixed in 1.123.43, 2.22.1, and 2.20.7.	N/A	More Details
CVE-2026-44791	n8n is an open source workflow automation platform. Prior to 1.123.43, 2.22.1, and 2.20.7, an authenticated user with permission to create or modify workflows could bypass the patch for CVE-2026-42232 in the XML node. When combined with other nodes, this could lead to RCE on the n8n host. This vulnerability is fixed in 1.123.43, 2.22.1, and 2.20.7.	N/A	More Details
	n8n is an open source workflow automation platform. Prior to 1.123.43, 2.22.1, and 2.20.7, an attacker with write access to the git repository connected to an n8n Source Control configuration		

CVE-2026-44792	could commit a malicious Data Table JSON file containing a crafted column name. When an administrator performed a Source Control Pull, n8n imported the file and could lead to SQL injection on the internal PostgreSQL instance. Exploitation requires the n8n instance uses PostgreSQL as its database backend, the Source Control feature is enabled and connected to a repository the attacker can write to, and an administrator triggers a Source Control Pull. This vulnerability is fixed in 1.123.43, 2.22.1, and 2.20.7.	N/A	More Details
CVE-2026-44956	Low-privileged users could use their Full Name as a vector for a stored XSS attack. The name is included in system-generated emails, whose content is stored in the details field of the userlog table. An admin user viewing the email content through userlog-details.php would have any malicious JavaScript payload executed due to missing output sanitisation. Proper escaping has been added to the userlog details output.	N/A	More Details
CVE-2026-44957	A missing access control check when invoking various modify methods in the XML-RPC API of Revive Adserver 6.0.6 and earlier. The API allowed entities to be reassigned to different parent entities, leading to inconsistent ownership relationships. This issue was exploitable only in combination with CVE-2026-34917 or with third-party API extensions that expose API functionality to low-privileged users. Access control checks have been added to validate access to parent entities in the API modify methods.	N/A	More Details
CVE-2026-44958	An access control bypass allows an advertiser-level user to activate or deactivate a banner in Revive Adserver 6.0.6 and earlier, even when such permissions were not granted. The banner-edit.php script allowed the banner status to be overwritten solely based on banner edit permissions. The status field has been removed from the hidden form fields in the banner edit screen.	N/A	More Details
CVE-2026-44959	A missing validation of user input exists when saving delivery limitations in Revive Adserver 6.0.6 and earlier. A low-privileged user could add an unexpected component parameter and inject malicious PHP code into the compiledlimitations field, which would then be executed during banner delivery. Input sanitisation has been improved to ensure that unexpected parameters are filtered out.	N/A	More Details
CVE-2026-44960	A stored XSS can be exploited by leveraging the usernames as an attack vector. When an admin user viewed the audit log details for affected entries, any malicious JavaScript payload embedded in the username would be executed due to missing output sanitisation. Proper escaping has been added to the audit log details output.	N/A	More Details
CVE-2026-44961	The XML-RPC API addUser method has a validation bypass introduced in the fix for CVE-2025-55129. As a result, API users could create usernames that enabled impersonation or stored XSS attacks. Proper validation has been added where it was missing.	N/A	More Details
CVE-2026-45732	n8n is an open source workflow automation platform. Prior to 1.123.43, 2.22.1, and 2.20.7, the OAuth1 and OAuth2 credential reconnect endpoints authorized access using credential:read rather than credential:update. An authenticated user with read-only access to a shared credential could initiate an OAuth reconnect flow and overwrite the stored token material for that credential with tokens bound to an external account they control. Workflows relying on the affected credential would subsequently execute under the attacker's OAuth identity, enabling data exfiltration to attacker-controlled external services and persistent takeover of shared integrations. This vulnerability is fixed in 1.123.43, 2.22.1, and 2.20.7.	N/A	More Details
CVE-2026-2467	Heap-based Buffer Overflow vulnerability in RTI Connext Professional (Core Libraries) allows Overflow Variables and Tags.This issue affects Connext Professional: from 7.4.0 before 7.7.0, from 7.0.0 before 7.3.1.3, from 6.1.0 before 6.1.*, from 6.0.0 before 6.0.*, from 5.3.0 before 5.3.*, from 5.0.0 before 5.2.*.	N/A	More Details
CVE-2026-48617	A flaw in Node.js Permission Model enforcement allows Bypass via `process.report.writeReport()` Path Misvalidation. This can lead to confidentiality impact or bypass of the intended security boundary under affected configurations. This vulnerability affects all supported release lines: **Node.js 22**, **Node.js 24**, and **Node.js 26**.	N/A	More Details
CVE-2026-47379	NocoDB is software for building databases as spreadsheets. Prior to 2026.05.1, the shared-view password check fell back to strict-equality (===) comparison for legacy plaintext passwords, leaking the password's length and per-character prefix through response timing. This vulnerability is fixed in 2026.05.1.	N/A	More Details
	UBB.threads is vulnerable to Stored XSS via user posts and user profile fields. The application		

CVE-2026-54219	fails to properly sanitize user input, allowing low privileged attackers to inject arbitrary JavaScript that executes in a victim's browser upon viewing. Because vendor contact attempts were unsuccessful, the vulnerability has only been confirmed in version 7.7.5 but may also affect other versions.	N/A	More Details
CVE-2026-12620	The GridTime 3000 GNSS Time Server leaks the access token in the URL parameters of some endpoints. This issue affects GridTime 3000: from 1.0r0.03 through 1.1r0.0.	N/A	More Details
CVE-2026-47388	NocoDB is software for building databases as spreadsheets. Prior to 2026.05.1, a low-privilege MCP token holder with knowledge of an attachment path could read any file in shared storage, including attachments belonging to other bases and workspaces, because the MCP readAttachment tool did not verify the file's ownership. This vulnerability is fixed in 2026.05.1.	N/A	More Details
CVE-2026-54220	uBB.threads is vulnerable to a Cross-Site Request Forgery (CSRF) due to a lack of protective mechanisms. This allows an attacker to trick an authenticated user into executing unintended actions. Because vendor contact attempts were unsuccessful, the vulnerability has only been confirmed in version 7.7.5 but may also affect other versions.	N/A	More Details
CVE-2026-47387	NocoDB is software for building databases as spreadsheets. Prior to 2026.05.1, the shared form-view submit handler (packages/nc-gui/composables/useSharedFormViewStore.ts) in NocoDB writes the form's redirect_url to window.location.href after a same-host check that does not validate the URL scheme. A user with editor role (or above) on any base can plant a javascript: URL in the form's redirect_url; when an authenticated viewer opens the share-link and submits the form, the payload executes in the NocoDB origin and can read the session token from localStorage["nocodb-gui-v2"]. This vulnerability is fixed in 2026.05.1.	N/A	More Details
CVE-2026-12621	Improper neutralization of input during web page generation XSS vulnerability in the GridTime 3000 (password reset form) allows XSS. This issue affects GridTime 3000: from 1.0r0.03 before 1.2r0.0.	N/A	More Details
CVE-2026-12622	The GridTime 3000 GNSS Time Server has an open redirect vulnerability in the password change form submission. This issue affects GridTime 3000: from 1.0r0.03 through 1.1r0.0.	N/A	More Details
CVE-2026-50221	In OpenStack Swift before 2.37.2, proxy-server does not strip internal update headers (X-Container-Host, X-Container-Device, X-Delete-At-Host, X-Delete-At-Device) from client requests before forwarding them to object-servers. An authenticated user with write access can inject these headers to redirect container update requests to an attacker-controlled server, enabling server-side request forgery. The SSRF requests expose internal cluster metadata including storage policy indexes, partition mappings, device names, and when at rest encryption is enabled, cipher text and initialization vectors for the container-level encryption key. The attacker can also cause "ghost listings" in arbitrary containers via the shard-range redirect mechanism.	N/A	More Details
CVE-2026-47386	NocoDB is software for building databases as spreadsheets. Prior to 2026.05.1, two concurrent token-exchange requests using the same OAuth authorization code could each mint a distinct valid (access_token, refresh_token) pair, breaking the single-use guarantee that PKCE relies on. This vulnerability is fixed in 2026.05.1.	N/A	More Details
CVE-2026-47385	NocoDB is software for building databases as spreadsheets. Prior to 2026.05.1, an authenticated user with base-create permission can attach a SQLite source pointing at an arbitrary file on the NocoDB host, including NocoDB's own internal databases. The SQLite client and the base/integration create services accepted a caller-supplied filename and passed it to fs.exists and fs.open('w') without restricting the location. A user could point a source at noco.db, at a tenant database under nc_minimal_dbs/, or at any writable path the NocoDB process can reach, and then read or overwrite its contents through the regular table APIs.This vulnerability is fixed in 2026.05.1.	N/A	More Details
CVE-2026-54316	Claude Code is an agentic coding tool. From 0.2.54 until 2.1.163, because the hostname huggingface.co was pre-approved as a bare hostname for the WebFetch tool, any path on that domain—including attacker-controlled model repositories—was auto-approved without a permission prompt or being subject to --allowedTools restrictions. An attacker able to inject untrusted content into a Claude Code context could direct it to issue WebFetch requests against attacker-controlled repository files (e.g. /resolve/main/config.json), which HuggingFace counts as downloads server-side, creating a covert out-of-band channel for encoding and exfiltrating data	N/A	More Details

	Claude can access such as files, environment variables, or command output. Reliably exploiting this required the ability to add untrusted content into a Claude Code context window. This vulnerability is fixed in 2.1.163.		
CVE-2026-54257	Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. From 42.3.1 until 42.3.3, Buffer performs incorrect byte length calculations resulting in heap buffer under/overflow. Most apps will crash and some may perform incorrect buffer allocations in the Node.js Buffer API resulting in unexpected truncation or allocation. This vulnerability is fixed in 42.3.3.	N/A	More Details
CVE-2026-47384	NocoDB is software for building databases as spreadsheets. Prior to 2026.05.1, an authenticated user with column-create permission can inject SQL into the bulk groupBy endpoint by setting a column's title to a SQL fragment. The bulk groupBy path in group-by.ts builds three database-specific knex.raw() aggregations that interpolate the request's column_name directly into the SQL string. Column lookup in data-table.service.ts matches on both the sanitized column_name field and the free-text title, so a title containing a SQL fragment bypasses the public endpoint's existing column allowlist and reaches the query builder unescaped. This vulnerability is fixed in 2026.05.1.	N/A	More Details
CVE-2026-54007	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.6, the chat message listener allows non-same-origin input:prompt and action:submit messages, so an external site can set prompt text and trigger submitPrompt() in an authenticated victim session. I validated this with a cross-origin attacker page that auto-posted messages and caused unauthorized POST /api/v1/chats/new and POST /api/chat/completions requests containing attacker-controlled prompts. This enables cross-site forced actions and model/tool execution under victim privileges without consent. This vulnerability is fixed in 0.9.6.	N/A	More Details
CVE-2025-71351	picklescan before 0.0.25 fails to detect malicious pickle files that use timeit.timeit() in the __reduce__ method, allowing remote code execution. Attackers can craft pickle files that import dangerous libraries like os and execute arbitrary system commands, which evade picklescan detection and execute when pickle.load() is called.	N/A	More Details
CVE-2026-9158	In Eclipse 4diac FORTE versions 3.0.0 to 3.1.0, a specially crafted DELETE connection command to the management interface can lead to a dangling pointer. This allows subsequent commands to access freed memory (use-after-free).	N/A	More Details
CVE-2026-47383	NocoDB is software for building databases as spreadsheets. Prior to 2026.05.1, an authenticated commenter could store HTML in row comments that executed as script when other users hovered over the comment in the expanded form view. The comment write paths persisted the raw comment body with no server-side sanitisation; the expanded-form sidebar then rendered the stored body and fed its data-tooltip attribute to Tippy with allowHTML: true. Even when the editor stripped script tags at write time, attribute-level payloads re-entered the DOM as live HTML on hover. This vulnerability is fixed in 2026.05.1.	N/A	More Details
CVE-2026-47382	NocoDB is software for building databases as spreadsheets. Prior to 2026.05.1, the connection-test endpoint opened a raw TCP socket to the user-supplied database host without resolving and range-checking the destination, so private and link-local addresses (including IPv4-mapped IPv6 forms and localhost) reached the driver. This vulnerability is fixed in 2026.05.1.	N/A	More Details
CVE-2026-54221	UBB.threads is vulnerable to Reflected XSS. The application improperly handles user input in certain requests, enabling attackers to execute arbitrary JavaScript in the context of a victim's browser by tricking them into clicking a crafted link. Because vendor contact attempts were unsuccessful, the vulnerability has only been confirmed in version 7.7.5 but may also affect other versions.	N/A	More Details
CVE-2026-53875	picklescan before 1.0.3 contains a scanning bypass vulnerability in the scan_pytorch function that allows attackers to embed malicious magic numbers via dynamic eval using the __reduce__ trick. Attackers can craft malicious PyTorch payloads that evade picklescan detection while remaining executable, enabling arbitrary code execution when loaded with torch.load().	N/A	More Details
CVE-2026-54222	UBB.threads is vulnerable to Blind SQL Injection, allowing attackers with access to the Members in Control Panel to interact with the underlying database. Due to insufficient input sanitization, an attacker can extract sensitive information, such as user credentials, by manipulating SQL queries through time-based or boolean-based techniques. Because vendor contact attempts were unsuccessful, the vulnerability has only been confirmed in version 7.7.5 but may also affect other versions.	N/A	More Details

CVE-2026-47381	NocoDB is software for building databases as spreadsheets. Prior to 2026.05.1, a user in one workspace could exercise another workspace's integration through the testConnection endpoint by supplying its ID, because the integration was fetched in a bypass scope and the caller's permission check matched any base in any workspace. This vulnerability is fixed in 2026.05.1.	N/A	More Details
CVE-2026-47380	NocoDB is software for building databases as spreadsheets. Prior to 2026.04.1, sign-in response timing differed between known and unknown email addresses because the unknown-user branch returned without performing a password hash comparison. This vulnerability is fixed in 2026.04.1.	N/A	More Details
CVE-2026-54224	UBB.threads is vulnerable to Denial of Service (DoS). By sending multiple concurrent requests to view any user profile on instances with many registered users, an authenticated attacker can easily exhaust database resources and completely deny access to the application for other users. Because vendor contact attempts were unsuccessful, the vulnerability has only been confirmed in version 7.7.5 but may also affect other versions.	N/A	More Details
CVE-2026-47377	NocoDB is software for building databases as spreadsheets. Prior to 2026.04.1, the client-side hashRedirect plugin called window.location.replace() on a path extracted from the URL hash fragment after only checking hashPath.startsWith('/'). Protocol-relative URLs (//attacker.com/...) also satisfy that check, so a crafted link silently redirected visitors to an attacker-controlled origin. This vulnerability is fixed in 2026.04.1.	N/A	More Details
CVE-2026-54223	UBB.threads is vulnerable to Path traversal, allowing attackers with privilege to edit templates to read and write any file on the application’s server that application has privileges to, what results in Remote Code Execution. Because vendor contact attempts were unsuccessful, the vulnerability has only been confirmed in version 7.7.5 but may also affect other versions.	N/A	More Details
CVE-2026-50193	jackson-databind contains the general-purpose data-binding functionality and tree-model for Jackson Data Processor. From 2.13.0 until 2.14.0, a potential Denial-of-Service exists when attacker sends deeply nested JSON if (and only if) the service reads deeply nested (1000s of levels) JSON as JsonNode (ObjectMapper.readTree()) and writes out same (or modifided) node using JsonNode.toString(). This can consume significant amount of resources with concurrent relatively small requests (1000 nested arrays is 2kB). This vulnerability is fixed in 2.14.0.	N/A	More Details
CVE-2026-50141	Woodpecker is a CI/CD engine. Starting in version 3.0.0 and prior to version 3.14.1, a vulnerability in Woodpecker CI's gRPC layer allowed any authenticated agent to impersonate any other agent on the same server by injecting a forged `agent_id` value into outgoing gRPC metadata. The server correctly verified the JWT token but then discarded the verified agent identity in favor of the client-supplied value. Version 3.14.1 patches the issue. As a workaround, disable org agents (`WOODPECKER_DISABLE_USER_AGENT_REGISTRATION=true`) and delete existing ones.	N/A	More Details
CVE-2026-40455	An SQL Injection vulnerability exists in LMS (LAN Management System) before commit 4cb30a7 within the "tarifflist.php" module due to insufficient sanitization of the POST "tg[]" parameter. The application directly concatenates user-supplied array values into an SQL query using "implode()", allowing authenticated attackers to perform Error-Based SQL injection and extract sensitive database information.	N/A	More Details
CVE-2026-12619	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Microchip GridTime 3000 allows Cross-Site Scripting (XSS). This issue affects GridTime 3000: from 1.0r0.03 through 1.1r0.0.	N/A	More Details
CVE-2026-55736	Improperly Controlled Modification of Dynamically-Determined Object Attributes vulnerability in ash-project ash allows a user to set the value of a private action argument that is intended to be controlled only by trusted server-side code. Action arguments declared with public?: false are meant to be set internally (for example via Ash.Changeset.set_private_argument/3) and must not be settable from end-user input. When a changeset is built from a parameter map, Ash filters out private arguments, but the filtering is incomplete. In the regular changeset path (for_create, for_update, for_destroy), private arguments are stripped only when the parameter key is an atom. When the key is a binary (string), as is the case for user-supplied parameters, the private argument is kept and the user controls its value. In the atomic path (Ash.Changeset.fully_atomic_changeset/4, also reached through atomic and bulk updates), private arguments are not stripped at all, regardless of whether the key is an atom or a binary. An attacker who can submit parameters to an action that defines a private argument can therefore inject a value for that argument. Depending on how the application uses the argument	N/A	More Details

	(for example an acting_user_id driving authorization or record ownership), this can lead to an integrity violation or privilege escalation. This issue affects ash: from 3.0.0 before 3.29.3.		
CVE-2025-10560	Worksnaps before version 1.6.20260201 contains hardcoded cloud credentials and related secret material in the Worksnaps client application binaries. The exposed credentials included AWS access keys, S3 bucket names, and related cloud access information. The originally exposed AWS credentials authenticated as the AWS account root identity and provided access to Worksnaps production cloud resources, including S3 buckets containing sensitive data such as screenshots of user desktops. An attacker with access to the affected client binaries could extract or recover the credentials and use them to access affected Worksnaps cloud resources.	N/A	More Details
CVE-2026-53931	NocoDB is software for building databases as spreadsheets. Prior to 2026.05.1, the spreadsheet-import endpoint axiosRequestMake could be used as a generic HTTP proxy. Before the fix it was reachable unauthenticated, and its URL-extension allowlist was a regex tested against the full URL string, so URLs whose query string ended in .csv satisfies the gate even though the underlying request is for another file. This vulnerability is fixed in 2026.05.1.	N/A	More Details
CVE-2026-53930	NocoDB is software for building databases as spreadsheets. Prior to 2026.05.1, the base-migration endpoint accepted a caller-supplied URL that the migration worker dereferenced without enforcing protocol or destination, allowing scheme abuse (file:, ftp:, etc.) and probing of internal HTTP destinations. This vulnerability is fixed in 2026.05.1.	N/A	More Details
CVE-2026-40456	An OS Command Injection vulnerability exists in LMS (LAN Management System) before commit 9fcb4de due to an IP address parameter being passed to the "exec()" function without proper validation, allowing attackers to execute arbitrary operating system commands.	N/A	More Details
CVE-2026-40457	A Reflected Cross-Site Scripting (XSS) vulnerability exists in LMS (LAN Management System) before commit 9c5651b in the "dbrecover.php" and "netremap.php" modules where unsanitized GET parameters are directly embedded into HTML output. This allows an attacker to inject arbitrary JavaScript when an authenticated user clicks a crafted link, provided the required conditions (such as a network defined in the system) are met.	N/A	More Details
CVE-2026-53929	NocoDB is software for building databases as spreadsheets. Prior to 2026.05.1, with NC_SECURE_ATTACHMENTS=true, an authenticated uploader could deliver .html or .svg attachments that the browser rendered inline from the NocoDB origin instead of forcing a download. The signed attachment handler stored response-header overrides under PascalCase keys (ResponseContentDisposition, ResponseContentType) while the controller that served the file read them under lowercase-hyphen names (response-content-disposition). The mismatch dropped the Content-Disposition: attachment header, leaving Express to auto-render .html, .svg, and similar inline. This vulnerability is fixed in 2026.05.1.	N/A	More Details
CVE-2026-53928	NocoDB is software for building databases as spreadsheets. Prior to 2026.05.1, a stolen refresh token survived a password-forgot flow and could be used to mint fresh JWTs even after the user reset their password. passwordChange and passwordReset deleted the user's refresh tokens, but passwordForgot only rotated token_version and revoked OAuth tokens — it did not call UserRefreshToken.deleteAllUserToken(user.id). An attacker holding a captured refresh cookie could still exchange it for a new access token after the victim triggered the recovery flow. This vulnerability is fixed in 2026.05.1.	N/A	More Details
CVE-2026-46554	NocoDB is software for building databases as spreadsheets. Prior to 2026.04.4, deleted API tokens continued to authenticate requests until their cache entry expired, because the auth cache was not invalidated by token value at deletion time. The API token deletion path removed the database row but did not evict the token-value keyed entry from the auth cache. The auth middleware therefore continued to accept the deleted token until the cache entry aged out, leaving a deletion-to-revocation window of up to three days. This vulnerability is fixed in 2026.04.4.	N/A	More Details
CVE-2026-48939	A vulnerability in the iCagenda extension for Joomla allows the upload of arbitrary files in the file attachment feature, ultimately resulting in PHP code upload and execution.	N/A	More Details
CVE-2026-53927	NocoDB is software for building databases as spreadsheets. Prior to 2026.05.1, the spreadsheet-fetch endpoint (axiosRequestMake) accepted URLs whose path contained a permitted extension anywhere in the string, and applied a hand-rolled regex blocklist that omitted 127.0.0.0/8 and 169.254.0.0/16, allowing the cloud-metadata endpoint to be reached with a crafted URL This	N/A	More Details

	vulnerability is fixed in 2026.05.1.		
CVE-2026-11982	Grav 2.0.0-rc.9 with Admin2 2.0.0-rc.14 contains a stored cross-site scripting (XSS) vulnerability in the Admin2 Pages API save flow.	N/A	More Details
CVE-2026-47279	NocoDB is software for building databases as spreadsheets. Prior to 2026.05.1, the public shared-view relation endpoints accepted a caller-supplied column ID without verifying that the column was visible in the shared view, so anyone holding a share UUID could read links from any LTAR column on the view's table — including columns the view owner had hidden. publicMmList, publicHmList, and relDataList already ensured that the requested column belonged to the view's model, but did not check the view-column entry's show flag. This vulnerability is fixed in 2026.05.1.	N/A	More Details
CVE-2026-50643	8cc is vulnerable to an Out-of-Bounds Read due to improper handling of #line directives and GNU linemarkers. The compiler accepts attacker-controlled filename and line number metadata and later uses it without validation when accessing source line arrays. By supplying invalid or oversized line numbers, an attacker can trigger out-of-bounds memory access and a crash. Maintainer of this project was notified early about this vulnerability, but didn't respond with the details of vulnerability or vulnerable version range. Version corresponding to the commit b480958 was tested and confirmed as vulnerable, other versions were not tested but might also be vulnerable.	N/A	More Details
CVE-2026-10687	Rejected reason: This CVE Record has been rejected by the Zephyr Project CNA. Subsequent analysis, confirmed with the fix author, determined that the addressed defect does not apply to any released version of Zephyr: the affected code path exists only in unreleased development code, and no released branch is affected. As no released version is affected, this identifier is withdrawn.	N/A	More Details
CVE-2025-32437	AutoGPT is a workflow automation platform for creating, deploying, and managing continuous artificial intelligence agents. Prior to 0.6.63, `MediaDurationBlock` will download and store the video in a temporary directory without deleting before all noded are done. `StepThroughItemsBlock` can be used to iterate `MediaDurationBlock` multiple times. `StepThroughItemsBlock` does not limit the number of loops. In addition, `MediaDurationBlock ` does not limit the amount of disk space consumed in the current working directory and does not delete the video after outputing the result. When a malicious user chooses to screen shot many web pages, the disk space will eventually run out, causing a DoS. Version 0.6.63 patches the issue.	N/A	More Details
CVE-2026-0864	When using the "configparser" module to write configuration files containing multi-line text values with carriage return characters (\r) the resulting file could be injected with unexpected keys and values if the attacker controls the written value.	N/A	More Details
CVE-2025-32436	AutoGPT is a workflow automation platform for creating, deploying, and managing continuous artificial intelligence agents. Prior to 0.6.63, `AddAudioToVideoBlock` will download and store the video and audio in a temporary directory without deleting before all noded are done. `StepThroughItemsBlock` can be used to iterate `MediaDurationBlock` multiple times. `StepThroughItemsBlock` does not limit the number of loops. In addition, `AddAudioToVideoBlock` does not limit the amount of disk space consumed in the current working directory and does not delete the video after outputing the result. When a malicious user chooses to screen shot many web pages, the disk space will eventually run out, causing a DoS. Version 0.6.63 patches the issue.	N/A	More Details
CVE-2025-32424	AutoGPT is a workflow automation platform for creating, deploying, and managing continuous artificial intelligence agents. Prior to 0.6.63, ScreenshotWebPageBlock will store the captured screenshots in a temporary directory. `StepThroughItemsBlock` can be used to iterate `ScreenshotWebPageBlock` multiple times. `StepThroughItemsBlock` does not limit the number of loops. In addition, `ScreenshotWebPageBlock` does not limit the amount of disk space consumed in the current working directory. When a malicious user chooses to screen shot many web pages, the disk space will eventually run out, causing a DoS. Version 0.6.63 patches the issue.	N/A	More Details
CVE-2026-	NocoDB is software for building databases as spreadsheets. Prior to 2026.05.1, revokeAllOAuthTokensByUser in the users service is an empty stub being called from passwordChange, passwordForgot, and passwordReset. OAuth access and refresh tokens were	N/A	More

53926	not revoked when the user changed, reset, or recovered their password, leaving an attacker-issued OAuth grant valid after the user believed they had locked the attacker out. This vulnerability is fixed in 2026.05.1.		Details
CVE-2025-32422	AutoGPT is a workflow automation platform for creating, deploying, and managing continuous artificial intelligence agents. Prior to 0.6.63, `StepThroughItemsBlock` can iterate all the contents in a list and send them to `FileStoreBlock` for downloading one by one. Although `FileStoreBlock` has access time limits for downloading files, `StepThroughItemsBlock` can be used to slowly iterate and download relatively small files (e.g., 100M) multiple times. `StepThroughItemsBlock` does not limit the number of loops. In addition, `FileStoreBlock` does not limit the amount of disk space consumed in the current working directory. When a malicious user chooses to download too many videos, the disk space will eventually run out, causing a DoS. Version 0.6.63 patches the issue.	N/A	More Details
CVE-2026-49336	@microsoft/kiota-http-fetchlibrary provides TypeScript libraries for Kiota-generated API clients. In versions 1.0.0-preview.97 through 1.0.0-preview.101, `@microsoft/kiota-http-fetchlibrary`'s `RedirectHandler` is documented as stripping `Authorization` and `Cookie` from cross-origin redirect targets, but the default `scrubSensitiveHeaders` callback in `RedirectHandlerOptions` uses case-sensitive property deletion (`delete headers.Authorization`, `delete headers.Cookie`) on a headers object that `FetchRequestAdapter.getRequestFromRequestInformation` has already lower-cased. The delete therefore targets keys that do not exist, the scrub is a no-op, and any Bearer token or Cookie attached by a kiota-generated SDK is forwarded to an attacker-controlled host across a 30x redirect. This is reachable in the default middleware chain (`MiddlewareFactory.getDefaultMiddlewares`) with no custom configuration, and applies to every kiota-generated TypeScript SDK that uses `BaseBearerTokenAuthenticationProvider` or any other authentication provider that sets the `Authorization` request header. Version 1.0.0-preview.102 patches the issue.	N/A	More Details
CVE-2026-12673	Liquidfiles versions before 4.2.12 are affected by a broken access control vulnerability resulting in privilege escalation from an Admin in a secondary domain to a Sysadmin by modifying a group in their managed secondary (non-default) group.	N/A	More Details
CVE-2025-32392	AutoGPT is a workflow automation platform for creating, deploying, and managing continuous artificial intelligence agents. Prior to 0.6.63, AutoGPT's LoopVideoBLock allows users to input a video file and process the video, such as looping it 5 times or extending the time, and finally writing it to disk. However, there is no limit on the resources that can be allocated during execution. For example, the number of loops is user-controllable and unlimited. When a malicious attacker loops too many times, the generated video is too large, and after writing it to disk, the disk space is exhausted, eventually causing DoS. Version 0.6.63 patches the issue.	N/A	More Details
CVE-2026-47376	NocoDB is software for building databases as spreadsheets. Prior to 2026.04.1, the password-reset page rendered the URL token directly into a JavaScript string literal in a server-rendered EJS template. EJS <%= %> HTML-entity-encodes a fixed set of characters but does not escape single quotes or backslashes, so a crafted token could break out of the JS string context and execute attacker-controlled script in the NocoDB origin. Triggering required only that a victim follow a malicious password-reset link. This vulnerability is fixed in 2026.04.1.	N/A	More Details
CVE-2026-8918	A permissive list of allowed inputs in ASUS Armoury Crate allows a local administrator to perform arbitrary memory read/write operations or cause a system crash (BSOD) by bypassing the validation mechanism.Refer to the ' Security Update for Armoury Crate App ' section on the ASUS Security Advisory for more information.	N/A	More Details
CVE-2026-12479	A path traversal vulnerability exists in keras-team/keras version 3.14.0, specifically in the `DiskIOStore.make` method within the Keras 3 model saving and loading library. This vulnerability arises from the improper handling of user-provided layer names, which are used to construct directory paths without sanitizing for parent directory components (`..`). While forward slashes (`/`) are restricted in layer names, directory traversal sequences are not. This allows an attacker to craft a malicious Keras model that, when saved or loaded, can escape the intended temporary working directory and perform unauthorized file system operations, such as creating directories or writing files in arbitrary locations.	N/A	More Details
CVE-2026-11940	tarfile.extractall() with the 'data' or 'tar' filter could be bypassed by a crafted archive where a hardlink references a symlink stored at a deeper name than the hardlink itself. The extraction fallback validated the symlink at it's archived location but recreated it at the hardlink's shallower path, letting a relative target the filter judged contained escape the destination directory. This	N/A	More Details

	allowed a malicious tar archive to create a symlink pointing outside the destination, enabling out-of-destination file reads or writes. This was an incomplete fix of CVE-2025-4330.		
CVE-2026-53632	launch-editor allows users to open files with line numbers in editor from Node.js. Prior to 2.14.1, the launch-editor NPM package accesses arbitrary paths including Windows UNC paths. When a UNC path is opened, Windows automatically attempts NTLM authentication to the remote host, causing the user's NTLMv2 password hash to be leaked to an attacker-controlled SMB server. This can result in credential compromise through offline hash cracking. This vulnerability is fixed in 2.14.1.	N/A	More Details
CVE-2026-11834	A command injection vulnerability has been identified in the DHCP option processing logic in multiple TP-Link router models, due to insufficient validation of externally supplied DHCP option data. An adjacent attacker may exploit this vulnerability by supplying crafted DHCP responses, potentially resulting in unauthorized command execution during device initialization or provisioning workflows. This typically occurs when the device is in a factory-default or unconfigured state. Successful exploitation may allow an adjacent, unauthenticated attacker to execute arbitrary commands with elevated privileges, potentially leading to full compromise of the affected device and unauthorized administrative control.	N/A	More Details
CVE-2024-27928	vantage6 is an open-source infrastructure for privacy preserving analysis. Prior to version 5.0.0, if an attacker hacks into a vantage6 user's email account, they can 1) reset the password via email and then 2) reset the 2FA token via email. This way they reduce 2FA to 1FA (email access). Note that most email providers require 2FA to access email, so this issue is not very likely to cause issues. Version 5.0.0 fixes the issue. No known workarounds are available.	N/A	More Details
CVE-2026-55602	http-proxy-middleware is node.js http-proxy middleware. From 0.16.0 until 2.0.10, 3.0.6, and 4.1.0, http-proxy-middleware documents router proxy-table entries as host, path, or host+path selectors, but the host+path implementation uses unanchored substring matching on attacker-controlled request metadata. As a result, a crafted Host header that is only a superstring match for a configured host+path key can still route a request to an unintended backend. This vulnerability is fixed in 2.0.10, 3.0.6, and 4.1.0.	N/A	More Details
CVE-2024-24769	vantage6 is an open-source infrastructure for privacy preserving analysis. Prior to version 5.0.0, users can reset their MFA token via API routes that send them an email. Currently the number of emails that is sent is not limited. This gives attackers the option to flood someones mailbox with a lot of emails, and would have adverse effects on the SMTP server which may be seen as spam sender. Note resetting the MFA token requires a correct password, so the potential impact for this is very low. Version 5.0.0 fixes the issue. No known workarounds are available.	N/A	More Details
CVE-2026-7166	Vulnerability involving the exposure of sensitive data provided without adequate protection. The API exposes email and phone number data from the 'email' and 'telefon' fields. This vulnerability is also present in the local database, as it contains accessible sensitive information such as data on minors and municipal users. Successful exploitation of this vulnerability could allow an unauthenticated remote attacker to gain access to sensitive information and data.	N/A	More Details
CVE-2026-7167	The vulnerability arises when the system fails to properly validate the 'email' field during the authentication process, allowing unverified or fake email addresses to be accepted. This lack of validation enables the creation of user accounts with fake email addresses, facilitating the mass creation of fraudulent accounts. Successful exploitation of this vulnerability could allow an authenticated attacker to carry out various attacks, such as mass spam distribution, system abuse, or bypassing user controls, thereby compromising the security and integrity of the system.	N/A	More Details
CVE-2026-48820	CakePHP is a rapid development framework for PHP. In versions 4.5.11 and earlier, 4.6.0 through 4.6.3, 5.0.0 through 5.1.6, 5.2.0 through 5.2.12, and 5.3.0 through 5.3.5, View::_getElementFileName() does not check that the resolved element path is within the application/plugin view template paths. When element names are created with specifically crafted user-supplied data this weakness can be leveraged to include other PHP files on the server. Patched releases are available in 5.3.6, 5.2.13, 5.1.7, 4.6.4, and 4.5.11.	N/A	More Details
CVE-2026-	Authelia is an open-source authentication and authorization server providing two-factor authentication and single sign-on (SSO) for applications via a web portal. In versions 4.38.0 through 4.39.19, when a user authenticates via Basic Auth (i.e via the `Authorization` header with the `Basic` scheme) on the authz verification endpoint, Authelia takes the username directly from the `Authorization` header and passes it as is to the regulation system for ban	N/A	More

47203	checking and attempt recording. LDAP treats usernames case insensitively : `john`, `John`, and `JOHN` all bind as the same user. But the regulation SQL queries treat the lookup of these values in certain scenarios as case sensitive. This allows each variation of a usernames case to have its own ban bucket. Upgrade to 4.39.20 to receive a patch. As a workaround, explicitly disable the basic auth mechanism.		Details
CVE-2026-54280	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to 3.14.1, payload resources are not closed correctly when a client disconnects in the middle of a write. If a payload is using an open file or similar limited resource, then an attacker may be able to cause resource starvation temporarily until garbage collection or similar closes the file. This vulnerability is fixed in 3.14.1.	N/A	More Details
CVE-2026-54279	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to 3.14.1, host-only cookies that are saved with CookieJar.save() and then restored later with CookieJar.load() lose their host-only status. This vulnerability is fixed in 3.14.1.	N/A	More Details
CVE-2026-54278	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to 3.14.1, during cleanup it is possible for a compressed request body to be decompressed into memory in one chunk. An attacker may be able to send a compressed payload in specific situations that could be decompressed into memory, potentially leading to DoS (a zip bomb edge case). This vulnerability is fixed in 3.14.1.	N/A	More Details
CVE-2026-54277	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to 3.14.1, it is possible to bypass the max_line_size check in parts of an HTTP request in the C parser. If using the optimised C parser (the default in pre-built wheels), then an attacker may be able to send oversized lines through the HTTP parser and use an excessive amount of memory, potentially leading to DoS. This vulnerability is fixed in 3.14.1.	N/A	More Details
CVE-2026-54276	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to 3.14.1, DigestAuthMiddleware can send an authentication response after following a cross-origin redirect. This likely requires an open redirect vulnerability or similar on the target domain for an attacker to be able to execute. Further, the attacker is only receiving the digest, so should only be able to extract the user's credentials if the cryptography is weak or there is some kind of password reuse. This vulnerability is fixed in 3.14.1.	N/A	More Details
CVE-2026-54275	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to 3.14.1, the server_hostname TLS SNI check can be bypassed when an existing connection is reused. If an application makes multiple requests to the same domain, but with different per-request server_hostname parameters, then the later calls may succeed by reusing the existing connection when they should have been rejected due to the TLS SNI check. This vulnerability is fixed in 3.14.1.	N/A	More Details
CVE-2026-54274	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to 3.14.1, if an attacker sends large incomplete websocket frame payloads, it may be possible to bypass the usual size limits on memory use. This vulnerability is fixed in 3.14.1.	N/A	More Details
CVE-2026-54273	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to 3.14.1, no limit was present on the number of pipelined requests that could be queued. An attacker may be able to use pipelined requests to use excessive amounts of memory, potentially leading to DoS. This vulnerability is fixed in 3.14.1.	N/A	More Details
CVE-2026-48989	Windows-MCP is an open-source project that integrates AI agents with Windows. In versions prior to 0.7.5, certain HTTP modes exposed the MCP control plane without authentication while enabling wildcard CORS (allow_origins=*, allow_methods=*, allow_headers=*). Because the same server also exposed a PowerShell tool that executes caller-controlled commands as the Windows user running Windows-MCP, attackers could reach the control plane from arbitrary origins or non-browser clients and achieve arbitrary PowerShell execution. This issue was fixed in version 0.7.5.	N/A	More Details
	The vulnerability is present in the ‘/addJugador’ endpoint: * The 'keyJugador' and 'keyJugadorObjectiu' parameters allow the modification of other users’ information without requiring prior authorization validation. This could enable an authenticated attacker to alter any user’s ID and change their information. * The ‘punts’ and ‘numObjectiusEliminats’ fields allow arbitrary data to be added because user input is not properly validated. This makes it possible to obtain authentic prizes, awarded by city councils, by falsifying game scores. * In the ‘tokens’		

CVE-2026-7165	field, administrative privileges can be self-assigned without server validation or prior authentication. This vulnerability could allow an authenticated attacker to grant themselves administrator permissions and thus escalate privileges. * Numeric fields allow the entry of extremely long values, which can cause the system to crash. Successful exploitation of this vulnerability could allow an authenticated attacker to launch a denial-of-service (DoS) attack, preventing created games from being playable. * The ‘urlImatge’ parameter allows server-side requests to arbitrary URLs, enabling the retrieval of users’ internal IP addresses, access to internal services, reading of local files, and unauthorized interaction with third-party APIs. An authenticated attacker could gain access to sensitive data.	N/A	More Details
CVE-2026-53778	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-12104	OS command injection in the environment and tunnel configuration functionality in SIMA GmbH Bondix through version 1.25.7.5 on Linux allows an authenticated attacker with configuration write access to execute arbitrary operating-system commands via crafted configuration values passed to server-side scripts.	N/A	More Details
CVE-2026-44727	Jupyter Server is the backend for Jupyter web applications. Prior to 2.20, the nbconvert HTTP handlers in jupyter_server render user-authored notebook HTML under the Jupyter origin without a sandbox directive in their Content-Security-Policy. Combined with nbconvert.HTMLExporter's default non-sanitizing behavior, a notebook carrying an HTML payload in a display_data output triggers stored XSS with cookie access, full /api/* authority, and kernel RCE. This vulnerability is fixed in 2.20.	N/A	More Details
CVE-2026-49468	LiteLLM is a proxy server (AI Gateway) to call LLM APIs in OpenAI (or native) format. Prior to 1.84.0, This vulnerability is fixed in 1.84.0.	N/A	More Details
CVE-2026-49461	pypdf is a free and open-source pure-python PDF library. Prior to 6.12.2, an attacker who uses this vulnerability can craft a PDF which leads to large memory usage. This requires extracting the text of a page which contains a form XObject with self-references. This vulnerability is fixed in 6.12.2.	N/A	More Details
CVE-2026-49460	pypdf is a free and open-source pure-python PDF library. Prior to 6.12.2, an attacker who uses this vulnerability can craft a PDF which leads to long runtimes. This requires accessing a stream which uses the /FlateDecode filter with a PNG predictor. This vulnerability is fixed in 6.12.2.	N/A	More Details
CVE-2026-47242	Net::IMAP implements Internet Message Access Protocol (IMAP) client functionality in Ruby. Prior to 0.6.5 and 0.5.15, when Net::IMAP#id is called with a hash argument, although the ID field value strings are correctly quoted (escaping quoted specials), they were not validated to prohibit CRLF sequences. While Net::IMAP#enable does process its arguments for aliases, it does not validate them as valid atoms (or as a list of valid atoms). The #to_s value is sent verbatim. Arguments to either command could be used by an attacker to inject arbitrary IMAP commands. This vulnerability is fixed in 0.6.5 and 0.5.15.	N/A	More Details
CVE-2026-47241	Net::IMAP implements Internet Message Access Protocol (IMAP) client functionality in Ruby. Prior to 0.6.5 and 0.5.15, several Net::IMAP commands accept a raw string argument which is only validated to prevent CRLF injection and then sent verbatim. If this string is derived from user-controlled input, an attacker can force the next command to be absorbed as a continuation of the first command. This will cause the first command to eventually fail, but also prevents it from returning until another command is sent (from another thread). That other command will not return until the connection is closed. This vulnerability is fixed in 0.6.5 and 0.5.15.	N/A	More Details
CVE-2026-47240	Net::IMAP implements Internet Message Access Protocol (IMAP) client functionality in Ruby. Prior to 0.6.5 and 0.5.15, several Net::IMAP commands accept a "raw data" argument that is sent verbatim after validation to prevent command injection. However, if a server does not support non-synchronizing literals, it may still be possible to inject arbitrary IMAP commands inside non-synchronizing literals. A server without support for non-synchronizing literals may interpret the "+}\r\n" as the end of a malformed command line and respond with a tagged BAD. In that case, the contents of the literal will be interpreted as one or more new pipelined commands, allowing a CRLF command injection attack to succeed. This affects criteria for #search and #uid_search; search_keys for #sort, #thread, #uid_sort, and #uid_thread; and attr for #fetch and #uid_fetch. This vulnerability is fixed in 0.6.5 and 0.5.15.	N/A	More Details

CVE-2026-45034	PhpSpreadsheet is a pure PHP library for reading and writing spreadsheet files. Prior to 1.30.5, CVE-2026-34084 was patched by the helper File::prohibitWrappers. The helper calls parse_url($filename, PHP_URL_SCHEME) and then checks is_string($scheme) && strlen($scheme) > 1 to reject stream wrappers such as phar://, php://, data:// or expect://. The check is not equivalent to "does the path contain a wrapper". When the input has the form phar:///path/file.phar/inner with three or more slashes after the scheme, parse_url returns boolean false instead of returning the scheme string. The is_string($scheme) branch is therefore skipped, the helper returns without throwing, and the caller proceeds. PHP's stream layer, however, still treats phar:///... as a valid phar wrapper and opens the underlying phar file. The result is that IOFactory::load($attackerPath) walks past the patch and still touches the phar wrapper. On PHP 7.x, simply reaching the phar wrapper via is_file is enough for PHP to automatically deserialize the phar metadata, which in turn invokes the magic methods __wakeup and __destruct of an attacker controlled object and gives full RCE. On PHP 8.x, automatic metadata deserialization for plain file ops was removed, so the chain at the PhpSpreadsheet layer reduces to a phar wrapper file read primitive, and RCE only resurfaces if the downstream consumer ever calls Phar::getMetadata. This vulnerability is fixed in 1.30.5.	N/A	More Details
CVE-2026-48931	A flaw in Node.js HTTP Agent can cause a client to accept as valid a response that is send before the client has sent the request. This vulnerability affects all supported release lines: **Node.js 22**, **Node.js 24**, and **Node.js 26**.	N/A	More Details
CVE-2026-44939	A command injection vulnerability in the Rancher Manager cluster before 2.14.2 import endpoint /v3/import/{token}_{clusterId}.yaml through unsanitized YAML parameters could allow remote attackers to break out of an image, and execute e.g. malicious containers.	N/A	More Details
CVE-2026-56138	AIL framework contains a path traversal vulnerability in the /objects/item/diff endpoint. The endpoint accepts item identifiers through the s1 and s2 query parameters and, prior to the fix, attempted to retrieve and compare item contents without first verifying that both referenced items existed as valid AIL objects. An authenticated AIL user could craft malicious item identifiers containing path traversal sequences to cause the application to read gzip-compressed files accessible to the AIL process. This could result in unauthorized disclosure of local file contents, limited to files readable by the application and compatible with the expected gzip-compressed item format. The issue was fixed by validating that both requested items exist before their contents are accessed.	N/A	More Details
CVE-2026-8296	In affected versions of Octopus Server with certain access levels it was possible to embed a Cross-Site Scripting Payload via artifacts.	N/A	More Details
CVE-2026-56448	A path traversal vulnerability exists in AIL Framework before the release containing commit 0041456af25da0cdea1c1c4624e46baff2731d8f. An authenticated AIL user can supply crafted object identifiers through the investigation workflow to cause file paths to resolve outside the intended image, favicon, or screenshot storage directories. This may allow the attacker to download and read arbitrary files that are accessible to the AIL process. The issue occurs because user-controlled path components were joined with application storage paths without verifying that the resolved path remained within the expected directory. The affected download functionality could then include the contents of such files in a generated archive.	N/A	More Details
CVE-2026-48794	Authelia is an open-source authentication and authorization server providing two-factor authentication and single sign-on (SSO) for applications via a web portal. In versions 4.36.0 through 4.39.19, due to lack of canonicalization of domains in very specific edge cases, an access control rule may be skipped when it should match a request. The specific conditions that could lead to a security issue for vulnerability are: 1. The specific target resource of the attack must be using the forwarded authorization integration; 2. The requested domain must have two additional segments compared to a session domain i.e. `a.b.example.com` is requested, but the session domain is `example.com`; 3. There access control rules must specify two separate rules which both contain inexact domain matches such as `*.b.example.com` and `*.example.com` i.e. wildcards, username matches, group matches; 4. The rules must be in order of most specific domain to least specific domain; 5. The second rule must be more permissive than the first rule; 6. The attacker must specifically request a URL for the more specific domain, with the second part containing one or more capitalized letters i.e. `https://a.B.example.com` and no other segment with capitalized letters; 7. The integration used must not be the Envoy ExtAuthz integration; and 8. The proxy must not canonicalize the requested host name in the relevant header before sending it to the relevant authorization endpoint. The kind of configuration used to produce this issue and result in a `bypass` rule being matched has long been highly	N/A	More Details

	discouraged. Essentially hosts which should be bypassed entirely should not be secured by having the proxy check them with the authorization handlers. Upgrade to 4.39.20 to receive a patch.		
CVE-2026-56450	AIL did not restrict repeated failed attempts to verify a two-factor authentication (OTP) code. An attacker who had reached the 2FA verification step, such as after successfully completing the password-authentication stage, could submit an unlimited number of OTP guesses. This could enable brute-force guessing of a valid code and bypass the intended second authentication factor, resulting in unauthorized account access. The patch introduces per-user failed-OTP tracking, blocks verification after 30 failed attempts for one hour, clears the counter after a successful OTP verification, and provides administrator recovery actions to purge affected lockouts.	N/A	More Details
CVE-2026-48787	gin-vue-admin is an AI-assisted basic development platform. In version 2.9.1, an authenticated attacker with access to the code-generation feature and MCP management interface can exploit this vulnerability by injecting attacker-controlled Go source code through POST /autoCode/addFunc, and then invoking POST /autoCode/mcpStart to trigger a rebuild and restart of the standalone MCP service. This allows arbitrary operating system commands to be executed on the server with the privileges of the application process. Successful exploitation may lead to remote code execution (RCE), modification of backend source code or runtime logic, deployment of persistent backdoors, access to or manipulation of application data and configuration, and further impact on local resources running under the same service account or privilege context. The risk is highest in deployments that retain the source tree, allow writes to source files, and support local build or startup of standalone MCP components. In environments using binary-only releases, read-only filesystems, or with local build capabilities removed, the exploitability of the full attack chain is significantly reduced. However, once the online code-generation capability and MCP-hosted startup workflow are enabled, the overall security impact may reach high to critical severity. As of time of publication, it is unknown if a patched version is available. As a workaround, enforce strict allowlist validation on path- and identifier-related fields such as `humpPackageName`, `packageName`, `FuncName`, and `Router`, and only permit safe identifier formats.	N/A	More Details
CVE-2026-6653	Use After Free in libxml2's xmlParseInternalSubset from GNOME libxml2 version 2.9.11 to 2.11.0 allows a remote attacker to cause a denial-of-service via maliciously crafted XML input with improper entity resolution handling.	N/A	More Details
CVE-2026-52911	In the Linux kernel, the following vulnerability has been resolved: ksmbd: scope conn->binding slowpath to bound sessions only When the binding SESSION_SETUP sets conn->binding = true, the flag stays set after the call so that the global session lookup in ksmbd_session_lookup_all() can find the session, which was not added to conn->sessions. Because the flag is connection-wide, the global lookup path will also resolve any other session by id if asked. Tighten the global lookup so that the returned session must have this connection registered in its channel xarray (sess->ksmbd_chann_list). The channel entry is installed by the existing binding_session path in ntlm_authenticate()/krb5_authenticate() when a SESSION_SETUP completes successfully, so this condition is a strict equivalent of "this connection has been accepted as a channel of this session". Connections that have not bound to a given session cannot reach it via the global table. The existing conn->binding gate for entering the slowpath is preserved so that non-binding connections keep the fast-path-only behavior, and the session->state check is unchanged.	N/A	More Details
CVE-2026-53571	Vite is a frontend tooling framework for JavaScript. Prior to 8.0.16, 7.3.5, and 6.4.3, the contents of files that are specified by server.fs.deny can be returned to the browser on Windows. Vite’s dev server denies direct access to sensitive files through server.fs.deny, including entries such as .env, .env.*, and *.{crt,pem}. However, on Windows, the deny logic does not correctly normalize NTFS ADS path forms before access checks are applied. Because of this, requests such as /.env::$DATA?raw are treated as allowed paths, while Windows resolves them to the original file's default data stream. Similar to that, Windows allows accessing a file using a different name with the 8.3 short name compatibility feature. Vite did not reject accessing files via them. This vulnerability is fixed in 8.0.16, 7.3.5, and 6.4.3.	N/A	More Details
CVE-2025-61028	An issue in the time_t_to_dt component of openlink virtuoso-opensource v7.2.11 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.	N/A	More Details

CVE-2026-50556	Angular is a development platform for building mobile and desktop web applications using TypeScript/JavaScript and other languages. Prior to 22.0.0-rc.2, 21.2.16, 20.3.24, and 19.2.25, a Cross-Site Scripting (XSS) vulnerability exists in @angular/platform-server's DOM emulation dependency (domino) when serializing the content of <noscript> elements. When rendering dynamic text content inside a <noscript> element via template bindings (such as {{ value }} or [textContent]), the template engine expects the browser to render the content safely. Under Server-Side Rendering (SSR), domino is configured with scripting enabled, meaning <noscript> is treated as a raw-text element. However, domino's serializer completely omitted <noscript> from the list of raw-text elements requiring closing-tag escaping during DOM serialization. As a result, any occurrence of </noscript> in the bound dynamic text was never escaped under any circumstances. The unescaped closing tag was serialized directly into the output HTML (e.g. <noscript></noscript><script>alert(1)</script></noscript>). When parsed by a browser, it closes the <noscript> block early, allowing the injected <script> block to execute in the user's browser context, causing same-origin Cross-Site Scripting (XSS). This vulnerability is fixed in 22.0.0-rc.2, 21.2.16, 20.3.24, and 19.2.25.	N/A	More Details
CVE-2026-4027	A security vulnerability has been identified in FlexNet Manager Suite 2025 R1 and R2 that could allow unauthorized access to attachment files due to insufficient access control.	N/A	More Details
CVE-2026-11942	Akaunting 3.1.21 contains an authenticated stored cross-site scripting vulnerability in the reusable delete confirmation flow. A user with permission to create or modify records, such as Items, can store HTML/JavaScript in the record name.	N/A	More Details
CVE-2026-48788	Remark42 is a self-hosted comment engine for blogs, articles, or any other place where readers can add comments. Versions 1.6.0 through 1.15.0 contain a Cross-Site Scripting (XSS) vulnerability exploitable through content-type spoofing. The Remark42 image proxy fetches an arbitrary remote URL and re-serves the response from Remark42's own origin. During the download phase, the proxy determines whether the resource is an image by inspecting only the Content-Type header advertised by the remote server, never examining the actual bytes; during the serving phase, it instead derives the response Content-Type by sniffing those bytes with http.DetectContentType. An attacker can exploit this inconsistency by hosting a URL that advertises Content-Type: image/png while returning an HTML/JavaScript body: the download check accepts it as an image, the serving path sniffs the body and emits Content-Type: text/html, and the browser renders the attacker-controlled HTML/JavaScript as a document within Remark42's origin. Exploitation requires no Remark42 account on the target instance; the attacker only needs to host the malicious upstream URL and deliver the proxy link to a victim by any means, such as email, direct message, or a link on another website. This issue has been fixed in version 1.16.0.	N/A	More Details
CVE-2026-54268	Angular is a development platform for building mobile and desktop web applications using TypeScript/JavaScript and other languages. Prior to 22.0.1, 21.2.17, and 20.3.25, a Denial of Service (DoS) vulnerability exists in the @angular/common package of the Angular framework. The formatDate function, which is also utilized by the standard Angular DatePipe, does not properly limit or validate the length of the format parameter. When parsing a maliciously crafted, excessively long date format string (e.g., a repeating pattern or very large string), the internal parser splits the string iteratively using a regular expression loop. This results in uncontrolled resource consumption (high CPU utilization and excessive memory allocations), leading to a Denial of Service (DoS). This vulnerability is fixed in 22.0.1, 21.2.17, and 20.3.25.	N/A	More Details
CVE-2026-54267	Angular is a development platform for building mobile and desktop web applications using TypeScript/JavaScript and other languages. Prior to 22.0.1, 21.2.17, and 20.3.25, to optimize client-side bootstrap in Server-Side Rendered (SSR) environments, Angular supports Hydration via provideClientHydration(). During SSR, Angular serializes the application's runtime state (such as cached HttpClient responses) and outputs it into the HTML stream as a <script> tag with a predictable identifier. During client bootstrap, Angular recovers this state by looking up the element via document.getElementById('ng-state') and parsing its text content. Because the DOM element lookup for the state container is predictable and relies solely on the ID selector (ng-state), it is susceptible to DOM Clobbering. If the application binds untrusted user input or CMS content to element properties such as id (e.g., <div [id]="userInput"> or <a id="ng-state">) before the genuine <script> tag is parsed by the browser, the attacker-controlled element takes precedence in the DOM lookup. During hydration, when Angular calls document.getElementById('ng-state'), the browser returns the attacker's clobbered element. Angular then attempts to parse the text content or attributes of this clobbered element as JSON. This vulnerability is fixed in 22.0.1, 21.2.17, and 20.3.25.	N/A	More Details

CVE-2026-54266	Angular is a development platform for building mobile and desktop web applications using TypeScript/JavaScript and other languages. Prior to 22.0.1, 21.2.17, and 20.3.25, Angular's HttpTransferCache caches HTTP requests made during Server-Side Rendering (SSR) so that they can be reused during client-side hydration. This avoids repeating the same HTTP requests on the client. The cached responses are stored in TransferState using a cache key generated by hashing request properties (method, response type, mapped URL, serialized body, and sorted query parameters). The cache keys are generated using a weak 32-bit DJB2-like polynomial rolling hash. The 32-bit hash space is extremely small, allowing attackers to find hash collisions. An attacker can easily find a query parameter string (e.g., q=aaCAZMMM for a search request) that produces the exact same 32-bit hash as a sensitive endpoint (e.g., /api/user/profile). When a victim visits a crafted link containing the colliding parameter, the SSR process executes both the search request and the profile request. Due to the hash collision, the search response overwrites the profile response in the TransferState cache. This vulnerability is fixed in 22.0.1, 21.2.17, and 20.3.25.	N/A	More Details
CVE-2026-54265	Angular is a development platform for building mobile and desktop web applications using TypeScript/JavaScript and other languages. Prior to 22.0.1, 21.2.17, and 20.3.25, an issue in the @angular/compiler package allows bypassing DOM property sanitization through the use of two-way property bindings. Specifically, when a native DOM property that requires sanitization (such as innerHTML, srcdoc, src, href, data, or sandbox) is bound using the two-way binding syntax (e.g., [(innerHTML)]="value" or bindon-innerHTML="value"), the Angular template compiler failed to apply the appropriate schema-derived sanitizer resolution to the TwoWayProperty operation. As a result, native two-way DOM bindings were emitted without the required sanitizer function, whereas equivalent one-way bindings would be properly sanitized. This flaw enables an attacker who can control the value of a two-way bound sensitive property to bypass Angular's built-in sanitization logic, potentially leading to client-side Cross-Site Scripting (XSS). This vulnerability is fixed in 22.0.1, 21.2.17, and 20.3.25.	N/A	More Details
CVE-2026-54264	Angular is a development platform for building mobile and desktop web applications using TypeScript/JavaScript and other languages. Prior to 22.0.1, 21.2.17, and 20.3.25, an information disclosure vulnerability exists in the @angular/service-worker package of the Angular framework. When the Service Worker fetches assets, it preserves metadata (such as headers) from the original request. However, on cross-origin redirects, the Service Worker fails to strip sensitive headers, violating the Fetch redirect algorithm. This allows a remote attacker to obtain sensitive credentials (e.g., Authorization tokens, Proxy-Authorization credentials, or session cookies) by triggering a cross-origin redirect to an untrusted external origin. This vulnerability is fixed in 22.0.1, 21.2.17, and 20.3.25.	N/A	More Details
CVE-2026-53655	node-tar is a full-featured Tar for Node.js. Prior to 7.5.16, tar (node-tar) applies a PAX extended header's size= record (and other PAX overrides) to the next header entry of any type, including intermediary metadata headers such as a GNU long-name (L) or long-link (K) entry. Per POSIX pax, a PAX extended header (x) describes the next file entry, not the intermediary extension headers that may sit between the x header and the file it annotates. Because node-tar lets the PAX size override the byte length of an intervening L/K/x header, an attacker can desynchronize node-tar's stream cursor relative to every other mainstream tar implementation (GNU tar, libarchive/bsdtar, Python tarfile, and the now-fixed tar-rs / astral-tokio-tar). The result is a tar parser interpretation differential (CWE-436): a single crafted archive yields a different set of members under node-tar than under the reference tar tools. An attacker can use this to hide a member from one parser while it is visible to another, which defeats security tooling whose scanner and extractor disagree on archive contents (e.g. a malware/secret scanner that lists entries with one library while a downstream step extracts with another) This vulnerability is fixed in 7.5.16.	N/A	More Details
CVE-2026-11943	Akaunting 3.1.21 contains an authenticated stored cross-site scripting vulnerability in the document timeline shown on invoice and bill detail pages. An authenticated user can store HTML/JavaScript in their own profile name.	N/A	More Details
CVE-2026-52725	Angular is a development platform for building mobile and desktop web applications using TypeScript/JavaScript and other languages. Prior to 22.0.0-rc.2, 21.2.15, 20.3.22, and 19.2.23, an issue in the @angular/core package allows bypassing script-execution restrictions during dynamic component creation. Specifically, the dynamic component instantiation mechanism (createComponent) failed to reject mounting components directly onto a <script> or namespaced script element (such as <svg:script>). This enabled the initialization of custom components on a tag that executes scripts, allowing attackers to hijack or inject script-executing	N/A	More Details

	hosts. This flaw enables an attacker who can control the host element or selector parameter passed to createComponent to initialize or mount an Angular component directly onto a <script> tag, leading to execution of untrusted code or client-side Cross-Site Scripting (XSS). This vulnerability is fixed in 22.0.0-rc.2, 21.2.15, 20.3.22, and 19.2.23.		
CVE-2026-50557	Angular is a development platform for building mobile and desktop web applications using TypeScript/JavaScript and other languages. Prior to 22.0.0-rc.2, 21.2.15, 20.3.22 and 19.2.22, an issue in the @angular/compiler and @angular/core packages allows bypassing element and attribute sanitization/validation through specific namespace workarounds. Specifically, namespaced script elements (e.g., <svg:script> or <:svg:script>) were not properly identified as script elements by the Angular template preparser, allowing them to pass through template compilation without being stripped. Furthermore, security context schema mappings for element attributes did not consistently handle attributes within namespaced elements (like SVG and MathML), opening up gaps where malicious namespaced attributes could bypass runtime and compile-time sanitizers. Combined, these flaws enable an attacker who can inject or supply a template/tag structure with custom namespaces to bypass Angular's script-stripping logic and attribute sanitizers, leading to client-side Cross-Site Scripting (XSS). This vulnerability is fixed in 22.0.0-rc.2, 21.2.15, 20.3.22 and 19.2.22.	N/A	More Details
CVE-2026-50178	The Angular Language Service VS Code Extension provides a rich editing experience for Angular templates. the client-side Angular Language Service VS Code extension configures the tooltip Markdown renderer with the isTrusted: true option (located in client/src/client.ts). This setting instructs VS Code to trust all rendered content it receives, which enables active elements such as command: URIs. However, the background Angular Language Server process fails to escape or sanitize brackets, raw links, and control characters from JSDoc strings before forwarding the hover Markdown content (located in server/src/handlers/hover.ts and server/src/text_render.ts). An attacker can leverage this behavior by crafting a project TypeScript or JavaScript file (or a third-party npm package dependency) containing a malicious JSDoc tooltip with an embedded active command link. When a developer hovers over the target symbol to render the tooltip and clicks the malicious link, the IDE executes the command sequence directly on the developer's host machine. Prior to 21.2.4, This vulnerability is fixed in 21.2.4.	N/A	More Details
CVE-2026-49241	The Angular Language Service VS Code Extension provides a rich editing experience for Angular templates. Prior to 21.2.4, the client-side Angular Language Service VS Code extension reads the custom TypeScript SDK paths typescript.tsdk and js/ts.tsdk.path directly from workspace configurations (.vscode/settings.json) without verifying VS Code Workspace Trust state or asking for user consent (located in client/src/client.ts). The client-side extension then passes the parsed settings path as a command-line argument (--tsdk) to the background Node.js language server process. During server initialization, the background language server resolves and dynamically imports (via standard Node.js require()) the module library tsserverlibrary.js relative to the workspace-specified custom directory path. An attacker can exploit this behavior by committing a repository containing a local malicious tsserverlibrary.js script inside a custom folder, and a crafted .vscode/settings.json file pointing to that folder. When a developer opens the repository folder in VS Code, the extension automatically attempts to initialize and load the server, which dynamically resolves, loads, and executes the malicious script silently in the background. This vulnerability is fixed in 21.2.4.	N/A	More Details
CVE-2026-41049	Incorrect caching of authentication between different users of the qSnapper dbus service before version 1.3.3 allowed any local attacker to use dbus functions after a privileged users has authenticated for them.	N/A	More Details
CVE-2026-41048	Incorrect caching of authentication between different polkit methods in qSnapper before version 1.3.3 allowed a local attacker to use functions like "restore from snapshot" even if only allowed to do "delete snapshot".	N/A	More Details
CVE-2026-41047	Lack of authentication when using the "snapshot diff" functions in qSnapper before version 1.3.3 allowed a local attacker to see otherwise read protected information.	N/A	More Details
	Backpropagate is a Python library for fine-tuning large language models on a single GPU. In versions 1.1.0 and 1.1.1, the optional Reflex web UI exposes a training control plane without authentication: dataset upload, model load, training start/stop, multi-run orchestration, GGUF export, and HuggingFace Hub push. The CLI accepts two operator-facing flags intended as security controls: --auth user:pass — documented as "require HTTP Basic authentication on every request to the UI." and--share — documented as "expose the UI on a public address;		

CVE-2026-48797	requires --auth." When --auth user:pass is passed, the CLI prints Auth: enabled (user: <username>) to confirm to the operator that authentication is active, then exports BACKPROPAGATE_UI_AUTH=user:pass to the subprocess that launches the Reflex backend. The Reflex backend (backpropagate/ui_app/**) never reads BACKPROPAGATE_UI_AUTH. No authentication middleware is registered. No request-level guard runs. No WebSocket upgrade guard runs. Any client that reaches the bound port — local or remote, depending on whether --share is used — has full UI access. An inline comment at backpropagate/cli.py:1217-1218 in the v1.1.0 source documents the gap: "For Phase 1 the variable is exported but Reflex doesn't read it yet." This comment was internal-facing; the user-facing documentation (README, CHANGELOG, SHIP_GATE) advertised the contract as enforced. An attacker who reaches the bound port can read uploaded datasets, trigger arbitrary training runs against any local base models as well as read their paths, trigger HuggingFace Hub pushes and cause disk-fill DoS. This issue has been fixed in version 1.2.0. If developers cannot immediately upgrade to 1.2.0 run backprop ui with no flags so it binds to localhost, use SSH port-forwarding (ssh -L 7860:localhost:7860 <training-host>) instead of --share for remote access, and audit any host previously launched with --share, re-issuing any HF tokens used during those sessions.	N/A	More Details
CVE-2026-49344	Mercator is an open source web application that enables mapping of the information system. Prior to version 2025.05.19, Mercator's Query Engine (`/admin/queries/execute`) accepts a JSON DSL (`from` / `select` / `filters` / `traverse` / `output`), translates it into an Eloquent query, and returns results as JSON. The controller method `QueryController::execute()` does not enforce an authorization gate, unlike `store()` and `massDestroy()` in the same controller which are correctly protected. As a result, any authenticated account — including the read-only Auditor role — can query models beyond its intended scope, including the `User` model. Additionally, the `password` column, although declared `$hidden`, is not excluded from filter predicates, which allows it to be used in `LIKE` conditions. The `schema()` and `schemaModel()` endpoints of the same controller are similarly unguarded. The Query Engine is read-only; integrity and availability are not affected. Version 2025.05.19 patches the issue.	N/A	More Details
CVE-2026-48929	Rocket.Chat in versions <8.5.1, <8.4.4, <8.3.6, <8.2.6, <8.1.6, <8.0.7, <7.13.9, and <7.10.13 is vulnerable to unauthenticated file deletion. The deleteFileMessage Meteor method permanently deletes any uploaded file by ID without requiring authentication. When called via an unauthenticated DDP WebSocket connection, Meteor.userId() returns null, causing the authorization check to be skipped. Execution falls through to FileUpload.getStore('Uploads').deleteById(fileID), which removes the file from storage and database unconditionally. File IDs are discoverable from public channel message payloads and download URLs.	N/A	More Details
CVE-2026-49357	Line Desktop MCP is a project that, while unaffiliated with the official line-bot-mcp-server, allows users to directly operate the LINE Desktop application on Windows or Mac via MCP. `line-desktop-mcp` supports a `--http-mode` Streamable HTTP transport for use with clients such as n8n. In this mode the server binds to `0.0.0.0` and exposes the MCP `/mcp` endpoint without an MCP-layer authentication check. Prior to version 1.1.2, any network client that can reach the port can initialize a session, list tools, and call tools that read LINE Desktop chat history or send LINE messages through the already logged-in desktop application. Version 1.1.2 fixes the issue.	N/A	More Details
CVE-2026-50555	Angular is a development platform for building mobile and desktop web applications using TypeScript/JavaScript and other languages. Prior to 22.0.0-rc.2, 21.2.16, 20.3.24, and 19.2.25, a Cross-Site Scripting (XSS) vulnerability exists in @angular/platform-server's DOM emulation dependency (domino) when serializing the content of raw-text elements (such as <script>, <style>, and <iframe>). domino supports escaping raw-text elements during serialization to prevent closing-tag breakout. However, a Unicode index alignment bug existed in this escaping logic. In JavaScript, string lengths and character indices are calculated based on UTF-16 code units (where astral characters—such as emojis—occupy 2 code units / 4 bytes). If the bound dynamic text contained astral Unicode characters before the closing tag (e.g. </script>, </style>, or </iframe>), the index offset calculation in domino's replacement logic shifted. This misalignment caused domino to fail to replace or escape the closing tag, leaving it raw and unescaped in the output HTML. An attacker who controls the dynamic text can supply a payload containing both an astral Unicode character and a closing tag (e.g., 😀</iframe><script>alert(1)</script>). When serialized on the server during SSR, the browser parses the unescaped closing tag, exits the raw-text context early, and executes the subsequent <script> block, leading to same-origin Cross-Site Scripting (XSS). This vulnerability is fixed in 22.0.0-rc.2, 21.2.16, 20.3.24, and 19.2.25.	N/A	More Details

CVE-2026-50269	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to 3.14.0, attacker-controlled input included into multipart/payload headers can be used to modify a request to inject additional headers or similar. In the unlikely situation that an application is passing user-controlled strings into MultipartWriter.append(headers=...) or Payload.headers, then an attacker may be able to modify the request to inject headers or change the contents of the request. This vulnerability is fixed in 3.14.0.	N/A	More Details
CVE-2026-50184	Angular is a development platform for building mobile and desktop web applications using TypeScript/JavaScript and other languages. Prior to 22.0.0-rc.2, 21.2.15, 20.3.22, and 19.2.23, an issue in the @angular/service-worker package compromises the integrity of request-policy enforcement during request reconstruction. When the Angular Service Worker intercepts network requests for matched assets, it reconstructs a new Request object using an internal helper function. During this reconstruction process, the helper function strips explicit client-defined safety parameters: the credentials configuration (such as credentials: 'omit') and the HTTP cache mode configuration (such as cache: 'no-store'). These are reverted back to standard browser-default parameters (credentials: 'same-origin' and default HTTP cache properties). This causes the browser to include active credentials (such as cookies or Authorization headers) on outbound requests where the client-side developer explicitly instructed they should be omitted, leading to potential session leaks. Additionally, it causes private or non-cacheable resources to be cached by the service worker's engine, making private page states accessible or persistent inside the client's local cache post-logout. This vulnerability is fixed in 22.0.0-rc.2, 21.2.15, 20.3.22, and 19.2.23.	N/A	More Details
CVE-2026-50171	Angular is a development platform for building mobile and desktop web applications using TypeScript/JavaScript and other languages. Prior to 22.0.0-rc.2, 21.2.15, 20.3.22, and 19.2.23, a Denial of Service (DoS) vulnerability exists in the @angular/common package of Angular. The formatNumber function, which is also utilized by DecimalPipe, PercentPipe, and CurrencyPipe, does not properly validate the upper bounds of the digitsInfo parameter. Specifically, the minimum and maximum fraction digits parsed from the digitsInfo string (e.g., 1.2-4) are converted to integers and used without limits. When parsing a maliciously crafted digitsInfo string with excessively large fraction digit values (e.g., 1.200000000-200000000), the internal roundNumber function attempts to pad the digits array to match the requested fraction size. This results in an unbounded loop that repeatedly pushes elements into an array. This vulnerability is fixed in 22.0.0-rc.2, 21.2.15, 20.3.22, and 19.2.23.	N/A	More Details
CVE-2026-50170	Angular is a development platform for building mobile and desktop web applications using TypeScript/JavaScript and other languages. Prior to 22.0.0-rc.2, 21.2.15, 20.3.22, and 19.2.23, a vulnerability was discovered in @angular/common when Server-Side Rendering (SSR) and hydration are enabled. The HttpTransferCache utility optimizes hydration by caching outgoing HTTP requests performed during SSR and transferring the cached state to the client-side application via TransferState. However, the caching mechanism fails to inspect the withCredentials flag or the Cookie header of outgoing requests. As a result, credentialed, user-specific responses may be cached by default in the shared TransferState payload. When these responses are serialized into the HTML, any caching layer (such as a CDN, reverse proxy, or shared server cache) that caches the SSR-rendered HTML page could inadvertently cache and leak one user's private data to other users, leading to a high-severity information disclosure vulnerability. This vulnerability is fixed in 22.0.0-rc.2, 21.2.15, 20.3.22, and 19.2.23.	N/A	More Details
CVE-2026-50169	Angular is a development platform for building mobile and desktop web applications using TypeScript/JavaScript and other languages. Prior to 22.0.0-rc.2, 21.2.15 20.3.22, and 19.2.23, an issue in the @angular/service-worker package compromises the integrity of request-policy enforcement during request reconstruction. When the Angular Service Worker intercepts network requests for matched assets, it reconstructs a new Request object using an internal helper function. During this reconstruction process, the helper function strips the strict, client-defined request redirect policy configuration (such as redirect: 'error'), falling back to the browser's default 'follow' strategy. If the target web application makes client-side requests with a strict policy (e.g., expecting a network error instead of automatically following redirects), the service worker will bypass this instruction and automatically follow HTTP 3xx redirects to other destinations. This acts as an unintended proxy/intermediary ("Confused Deputy") and can result in cookie/credential exposure or same-origin session-restricted data leakage if public dynamic routes redirect to sensitive routes. This vulnerability is fixed in 22.0.0-rc.2, 21.2.15, 20.3.22, and 19.2.23.	N/A	More Details
	Angular is a development platform for building mobile and desktop web applications using		

CVE-2026-50168	TypeScript/JavaScript and other languages. Prior to 22.0.0-rc.2, 21.2.15, 20.3.22, and 19.2.23, an issue in the @angular/platform-server package allows remote attackers to bypass host allowlist constraints and direct server-side outgoing requests to arbitrary external endpoints. This occurs due to a parser differential between the strict WHATWG URL parser used for allowlist validation and the lenient Domino URL parser used to initialize the server emulated DOM. When a server-side request contains a malformed URL with a double port structure (e.g., http://evil.com:80:80/path), Node's strict URL.canParse(url) logic returns false and skips host check validation entirely. However, the same malformed URL is later accepted and parsed leniently by Domino's internal parser, which resolves the origin to http://evil.com:80. The Angular SSR HTTP request interceptor (relativeUrlsTransformerInterceptorFn) then resolves all relative backend HTTP requests against this adopted origin, executing the SSRF attack. This vulnerability is fixed in 22.0.0-rc.2, 21.2.15, 20.3.22, and 19.2.23.	N/A	More Details
CVE-2026-46417	Angular is a development platform for building mobile and desktop web applications using TypeScript/JavaScript and other languages. Prior to 22.0.0-next.12, 21.2.13, 20.3.21, and 19.2.22, a Server-Side Request Forgery (SSRF) vulnerability exists in @angular/platform-server. The issue stems from how the server-side rendering (SSR) engine processes the request URL provided to the rendering entry points. When an absolute-form URL (e.g., http://evil.com) is passed to the rendering engine, the internal ServerPlatformLocation can be manipulated into adopting the attacker-controlled domain as the "current" hostname. Consequently, any relative HttpClient requests or PlatformLocation.hostname references are redirected to the attacker controlled server, potentially exposing internal APIs or metadata services. This vulnerability is fixed in 22.0.0-next.12, 21.2.13, 20.3.21, and 19.2.22.	N/A	More Details
CVE-2026-8934	A Missing Authorization vulnerability in a GraphQL private API operation of the Google App Engine section of the Cloud Console allows an unauthenticated remote attacker to leak sensitive App Engine request logs from other projects using a specially crafted request. This vulnerability was patched on 7 April 2026, and no customer action is needed.	N/A	More Details
CVE-2026-27868	An attacker with access via network to the Regesta Smart HD-PLC of the provider Teldat (in this case, NO registration action is required) who has the vulnerable software could obtain privilege information by using the command Version via the path: /upgrade/query.php?cmd=p+3&3Bversion resulting in a information disclosure. This issue affects Regesta Smart HD-PLC - TLDPH16D2: 11.02.05.10.02.	N/A	More Details
CVE-2026-11994	Akaunting 3.1.21 contains an authenticated stored Cross-Site Scripting vulnerability in the report management workflow. A user with permission to create or update reports can store arbitrary HTML/JavaScript in the description field of a report.	N/A	More Details
CVE-2026-11825	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2026-4026	A security vulnerability has been identified in FlexNet Manager Suite 2025 R1 that could allow an authenticated user with read-only access to account settings to escalate their privileges to Administrator level.	N/A	More Details
CVE-2026-27869	An attacker with access via network to the Regesta Smart HD-PLC of the provider Teldat (in this case, NO registration action is required) who has the vulnerable software could, with a Slow Loris attack, cause Denial of Service (DoS) on the web interface of the device. This issue affects Regesta Smart HD-PLC - TLDPH16D2: 11.02.05.10.02.	N/A	More Details
CVE-2026-27870	An attacker with access via network to the Regesta Smart HD-PLC of the provider Teldat (in this case, registration action IS required) who has the vulnerable software could, introduce arbitrary JavaScript by injecting a Cross-site Scripting (XSS) payload into the 'Hostname' field of the configuration file resulting in a XSS in the path /upgrade/query.php?cmd=p+3%3Bversion. This issue affects Regesta Smart HD-PLC - TLDPH16D2: 11.02.05.10.02.	N/A	More Details
CVE-2026-49345	Mercator is an open source web application that enables mapping of the information system. Prior to version 2025.05.19, a Server-Side Request Forgery (SSRF) vulnerability exists in Mercator's CVE configuration panel (`/admin/config/parameters`). The `testProvider()` method in `ConfigurationController` passes user-supplied input directly to `curl_init()` without validating the scheme, hostname, or destination IP address. An authenticated user with the `configure` permission can force the Mercator server to issue arbitrary outbound network requests. The suffix `/api/dbInfo` appended to the URL can be bypassed by injecting a `#` fragment character (e.g. `http://TARGET/PATH#`), allowing full control over the target URL. No scheme whitelist,	N/A	More Details

	host whitelist, or private/loopback IP block is applied. The `telnet://` scheme can be used for internal port scanning; the `gopher://` scheme enables interaction with unauthenticated internal services (Redis, Memcached), potentially leading to Remote Code Execution under specific deployment conditions. Version 2025.05.19 patches the issue.		
CVE-2026-54530	pypdf is a free and open-source pure-python PDF library. Prior to 6.13.0, an attacker who uses this vulnerability can craft a PDF which leads to an infinite loop. This requires extracting the text in layout mode. This vulnerability is fixed in 6.13.0.	N/A	More Details
CVE-2026-54531	pypdf is a free and open-source pure-python PDF library. Prior to 6.13.0, an attacker who uses this vulnerability can craft a PDF which leads to an infinite loop. This requires merging a file with outlines into a writer. This vulnerability is fixed in 6.13.0.	N/A	More Details
CVE-2026-54651	pypdf is a free and open-source pure-python PDF library. Prior to 6.13.1, an attacker who uses this vulnerability can craft a PDF which leads to an infinite loop. This requires merging a file with threads/articles into a writer. This vulnerability is fixed in 6.13.1.	N/A	More Details
CVE-2026-8317	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2025-62180	Pega Platform versions 8.3.0 through Infinity 25.1.2 are affected by an authorization weakness that may allow authenticated users to access certain additional data via crafted URLs.	N/A	More Details
CVE-2026-48616	Rocket.Chat versions <8.5.1, 8.4.4, 8.3.6, 8.2.6, 8.1.6, 8.0.7, 7.13.9, 7.10.13 has an access control vulnerability in Livechat files. Protected file downloads at /file-upload/:fileId/:name authorize livechat access using rc_room_type=l with rc_rid+rc_token, but the authorization path does not verify that rc_rid matches the requested file's rid. Furthermore, :fileId is predictable via sequential MongoDB IDs, and :name can be anything, allowing unauthenticated discovery of all uploaded files.	N/A	More Details
CVE-2026-28496	FOSSBilling is a free, open-source billing and client management system. Versions prior to 0.8.0 have a Server-Side Template Injection (SSTI) vulnerability in the template rendering system. Administrators with access to features that render Twig templates (email templates, mass mail campaigns, custom payment adapters, and the `string_render` API endpoint) can inject arbitrary Twig expressions, leading to information disclosure and remote code execution. The vulnerability exists because Twig templates are rendered without a sandbox, allowing access to the full Twig environment, API context, and the application's dependency injection container. Version 0.8.0 patches the issue. Some workarounds are available. Audit existing email templates for suspicious Twig expressions, rotate all admin and client API tokens, and/or block external access to /api/system/* at reverse proxy/WAF to mitigate chaining with GHSA-78x5-c8gw-8279.	N/A	More Details
CVE-2026-27604	FOSSBilling is a free, open-source billing and client management system. Starting in version 0.5.4 and prior to version 0.8.0, an authorization bypass in the API role handling allows unauthenticated access to privileged `/api/system/*` endpoints. Because `system` resolves to the cron admin identity, attackers can invoke admin API methods without valid credentials, session, or CSRF token. Version 0.8.0 patches the issue. Some workarounds are available. Block external access to `/api/system/*` at reverse proxy/WAF, restrict API access by trusted source IPs only (`api.allowed_ips`), rotate all admin/client API tokens immediately, invalidate active sessions and reset high-privilege credentials, and/or review API request logs for suspicious `/api/system/` access and treat as potential incident.	N/A	More Details
CVE-2026-3894	Out-of-bounds Read vulnerability in RTI Connext Professional (Core Libraries) allows Overread Buffers.This issue affects Connext Professional: from 7.4.0 before 7.7.0, from 7.0.0 before 7.3.1.3, from 6.1.0 before 6.1.*, from 6.0.0 before 6.0.*, from 5.3.0 before 5.3.*, from 5.0.0 before 5.2.*.	N/A	More Details
CVE-2026-11772	DRIMO CMS is vulnerable to Reflected XSS via q parameter in searching functionality. An attacker can prepare an URL that, when opened, results in arbitrary JavaScript execution in the victim's browser. Product is in End Of Life phase and will not receive any updates. However, deleting info.php file mitigates the vulnerability,	N/A	More Details
	Improper Neutralization of Script in Attributes in a Web Page vulnerability in pragdave earmark allows stored cross-site scripting via unescaped HTML attribute values. 'Elixir.Earmark.Transform':_make_att1/2 in lib/earmark/transform.ex splices attribute values		

CVE-2026-48591	verbatim between two literal " bytes: [" ", name, "=\"", value, "\""]. Text nodes are routed through the existing escape function which encodes " as ", but attribute values never visit that path. A markdown link whose URL or title contains a bare " closes the attribute early and lets the trailing bytes be parsed by the browser as fresh HTML attributes. For example, [click](http://example.com/?a=x" onerror="alert(1)) renders as click, executing arbitrary JavaScript in the victim's browser. The earmark library is no longer maintained and has been retired on Hex. No patched version will be released. All releases from 1.4.1 onward are affected, and users should migrate to a maintained Markdown library such as MDEx. This issue affects earmark from 1.4.1 onward.	N/A	More Details
CVE-2026-2842	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2026-48908	A vulnerability in SP Page Builder for Joomla allows unauthenticated users to upload arbitrary files, ultimately resulting in the upload and execution of PHP code.	N/A	More Details
CVE-2026-56275	Flowise before 3.1.0 contains a server-side request forgery vulnerability in the Execute Flow node that allows attackers to bypass security validation by providing intranet addresses through the base URL field. Attackers can initiate HTTP requests to internal network addresses, access cloud metadata, and enumerate internal services by exploiting the missing secureFetch verification in httpSecurity.ts.	N/A	More Details
CVE-2026-53876	RadiX AX6600 WiFi 6 Tri-Band Gaming Router contains an OS command injection vulnerability, which may lead to arbitrary command execution with the root privilege by a user who logs in to the web console as an administrator.	N/A	More Details
CVE-2026-12569	A critical remote code execution (RCE) vulnerability has been reported in PTC Windchill PDMlink and PTC FlexPLM. The vulnerability may be exploited through the deserialization of untrusted data. * This advisory also applies to all CPS versions * The identified vulnerability also impacts Windchill and FlexPLM releases prior to 11.0 M030	N/A	More Details
CVE-2026-7300	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in RTI Connext Professional (Web Integration Service) allows Filter Failure through Buffer Overflow.This issue affects Connext Professional: from 7.4.0 before 7.*, from 7.0.0 before 7.3.1.3, from 6.1.2 before 6.1.*.	N/A	More Details
CVE-2026-52910	In the Linux kernel, the following vulnerability has been resolved: bpf: Free reuseport cBPF prog after RCU grace period. Eulgyu Kim reported the splat below with a repro. [0] The repro sets up a UDP reuseport group with a cBPF prog and replaces it with a new one while another thread is sending a UDP packet to the group. The reuseport prog is freed by sk_reuseport_prog_free(). bpf_prog_put() is called for "e"BPF prog to destruct through multiple stages while cBPF prog is freed immediately by bpf_release_orig_filter() and bpf_prog_free(). If a reuseport prog is detached from the setsockopt() path (reuseport_attach_prog() or reuseport_detach_prog()), sk_reuseport_prog_free() is called without waiting for RCU readers to complete, resulting in various bugs. Let's defer freeing the reuseport cBPF prog after one RCU grace period. Note "e"BPF prog is safe as is unless the fast path starts to touch fields destroyed in bpf_prog_put_deferred() and __bpf_prog_put_noref(). [0]: BUG: KASAN: vmalloc-out-of-bounds in reuseport_select_sock+0xedc/0x1220 net/core/sock_reuseport.c:596 Read of size 4 at addr ffffc9000051e004 by task slowme/10208 CPU: 6 UID: 1000 PID: 10208 Comm: slowme Not tainted 7.0.0-geb7ac95ff75e #32 PREEMPT(full) Hardware name: QEMU Ubuntu 24.04 PC v2 (i440FX + PIIX, arch_caps fix, 1996), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 Call Trace: <IRQ> 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 reuseport_select_sock+0xedc/0x1220 net/core/sock_reuseport.c:596 udp4_lib_lookup2+0x3bc/0x950 net/ipv4/udp.c:495 __udp4_lib_lookup+0x768/0xe20 net/ipv4/udp.c:723 __udp4_lib_lookup_skb+0x297/0x390 net/ipv4/udp.c:752 __udp4_lib_rcv+0x1312/0x2620 net/ipv4/udp.c:2752 ip_protocol_deliver_rcu+0x282/0x440 net/ipv4/ip_input.c:207 ip_local_deliver_finish+0x3bb/0x6f0 net/ipv4/ip_input.c:241 NF_HOOK+0x30c/0x3a0 include/linux/netfilter.h:318 NF_HOOK+0x30c/0x3a0 include/linux/netfilter.h:318 __netif_receive_skb_one_core net/core/dev.c:6181 [inline] __netif_receive_skb net/core/dev.c:6294 [inline] process_backlog+0xaa4/0x1960 net/core/dev.c:6645 __napi_poll+0xae/0x340 net/core/dev.c:7709 napi_poll net/core/dev.c:7772 [inline]	N/A	More Details

	net_rx_action+0x5d7/0xf50 net/core/dev.c:7929 handle_softirqs+0x22b/0x870 kernel/softirq.c:622 do_softirq+0x76/0xd0 kernel/softirq.c:523 </IRQ> <TASK> __local_bh_enable_ip+0xf8/0x130 kernel/softirq.c:450 local_bh_enable include/linux/bottom_half.h:33 [inline] rcu_read_unlock_bh include/linux/rcupdate.h:924 [inline] __dev_queue_xmit+0x1dd7/0x3710 net/core/dev.c:4890 neigh_output include/net/neighbour.h:556 [inline] ip_finish_output2+0xca9/0x1070 net/ipv4/ip_output.c:237 NF_HOOK_COND include/linux/netfilter.h:307 [inline] ip_output+0x29f/0x450 net/ipv4/ip_output.c:438 ip_send_skb+0x45/0xc0 net/ipv4/ip_output.c:1508 udp_send_skb+0xb04/0x1510 net/ipv4/udp.c:1195 udp_sendmsg+0x1a71/0x2350 net/ipv4/udp.c:1485 sock_sendmsg_nosec net/socket.c:727 [inline] __sock_sendmsg net/socket.c:742 [inline] __sys_sendto+0x554/0x680 net/socket.c:2206 __do_sys_sendto net/socket.c:2213 [inline] __se_sys_sendto net/socket.c:2209 [inline] __x64_sys_sendto+0xde/0x100 net/socket.c:2209 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0x160/0xf80 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x415a2d Code: b3 66 2e 0f 1f 84 00 00 00 00 00 66 90 f3 0f 1e fa 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 b8 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f6bc31e41e8 EFLAGS: 00000212 ORIG_RAX: 000000000000002c RAX: ffffffffffffffda RBX: 00007f6bc31e4cdc RCX: 0000000000415a2d RDX: 0000000000000001 RSI: 00007f6bc31e421f RDI: 0000000000000003 RBP: 00007f6bc31e4240 R08: 00007f6bc31e4220 R09: 0000000000000010 R10: 0000000000000000 R11: ---truncated---		
CVE-2026-54892	Inefficient algorithmic complexity in Plug's nested-parameter decoder allows an unauthenticated remote attacker to cause denial of service. Plug.Conn.Query.decode/4 (and Plug.Conn.Query.decode_each/2) parse query strings and application/x-www-form-urlencoded request bodies. When a key contains many bracketed segments such as a[a][a][a]=1, the decoder walks the brackets and, for each of the N levels, performs a map operation keyed on an ever-growing binary prefix of the key, hashing the full byte range at each step. The total decode cost is therefore quadratic in the number of nesting levels. With the default Plug.Parsers.URLENCODED body limit of 1,000,000 bytes, a single request can carry roughly 333,000 nesting levels and saturate a BEAM scheduler for minutes. A small number of concurrent requests can saturate all schedulers and render a Plug-based server unresponsive. No authentication or knowledge of application routes is required. This vulnerability is associated with program files lib/plug/conn/query.ex and program routines Plug.Conn.Query.decode/4, Plug.Conn.Query.decode_each/2, Plug.Conn.Query.split_keys/6, Plug.Conn.Query.insert_keys/3, and Plug.Conn.Query.finalize_pointer/2. This issue affects plug from 1.15.0 before 1.15.5, 1.16.4, 1.17.2, 1.18.3, and 1.19.3.	N/A	More Details
CVE-2025-4994	The SafeLine SL6 and SL6+ devices integrated into elevator emergency intercom systems are vulnerable to an authentication bypass. This vulnerability allows attackers to bypass authentication requirements and access the device's configuration service via the Bluetooth Low Energy (BLE) interface. Consequently, an attacker within wireless range can gain unauthorized administrative access to the device configuration.	N/A	More Details
CVE-2026-44089	Totolink EX1200L router is vulnerable to Buffer Overflow in the login functionality in cgi-bin/cstecgi.cgi endpoint. This vulnerability could be exploited to cause the program to crash and to execute code remotely. This allows the attacker to perform actions as root including reading and editing data, as well as bricking the router. Because vendor contact attempts were unsuccessful, the vulnerability has only been confirmed in version 9.3.5u.6146_B20201023 but may also affect other versions.	N/A	More Details
CVE-2026-48909	SP LMS (com_splms) < 4.1.4 by JoomShaper deserializes user-controlled cookie data without validation, enabling an unauthenticated remote attacker to execute arbitrary code on the server.	N/A	More Details
CVE-2026-54303	n8n is an open source workflow automation platform. Prior to 2.24.0, an endpoint in the Meta and Microsoft Teams trigger nodes reflects a query parameter into the HTTP response without sanitization or Content-Security-Policy headers, enabling reflected XSS in the n8n origin when a logged-in user visits a crafted URL. This vulnerability is fixed in 2.24.0.	N/A	More Details
CVE-2026-	n8n is an open source workflow automation platform. Prior to 2.25.7 and 2.26.2, when @n8n/mcp-browser is run in HTTP transport mode, the MCP endpoint accepts session initialization and tool invocation requests without any authentication. Any network-reachable client, or any website visited by the user, can establish an MCP session and invoke browser-control tools. Where the n8n AI Browser Bridge extension is installed and a browser connection	N/A	More Details

54309	is active, an unauthenticated caller can access browser-control capabilities including navigation, JavaScript evaluation, and cookie and storage access against the user's real browser profile. This issue only affects instances where @n8n/mcp-browser is run with the HTTP transport (--transport http). This vulnerability is fixed in 2.25.7 and 2.26.2.		
CVE-2026-5366	Prefect version 3.6.23 is vulnerable to remote code execution due to improper handling of user-controlled input in the `GitRepository` storage class. The `commit_sha` parameter, which is passed to git commands, lacks validation and does not include a `--` separator to distinguish user input from git flags. This allows attackers to inject arbitrary git flags, such as `--upload-pack`, enabling execution of external programs. Additionally, the `directories` parameter can be exploited to inject git flags during sparse-checkout operations. These vulnerabilities allow any user with deployment creation permissions to execute arbitrary commands on worker machines, compromising shared work pools in multi-tenant environments.	N/A	More Details
CVE-2025-61027	An issue in the t_set_push component of openlink virtuoso-opensource v7.2.11 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.	N/A	More Details
CVE-2026-12475	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2025-61023	An issue in the st_compare component of openlink virtuoso-opensource v7.2.11 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.	N/A	More Details
CVE-2026-6645	An insecure process execution vulnerability exists in the pc-printer-updater.exe component of the PaperCut Print Deploy Client for Windows. The application, which typically operates with high-level system privileges, attempts to perform an internal validation check by invoking a secondary system utility using an unqualified file reference. Because the application does not specify an absolute path to this utility, it relies on the operating system's default search order to locate the executable. Under specific conditions, a local attacker with the ability to modify directories within the system's search path could plant a malicious binary that mimics the expected utility. This could result in the malicious code being executed with SYSTEM privileges, leading to a full compromise of the affected host.	N/A	More Details
CVE-2025-61021	An issue in the sqlo_natural_join_cond component of openlink virtuoso-opensource v7.2.11 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.	N/A	More Details
CVE-2025-61019	An issue in the sqlo_key_part_best component of openlink virtuoso-opensource v7.2.11 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.	N/A	More Details
CVE-2026-30799	Missing Authentication for Critical Function vulnerability in RTI Connext Professional (Security Plugins) allows Identity Spoofing.This issue affects Connext Professional: from 7.4.0 before 7.7.0, from 7.0.0 before 7.3.*, from 6.1.0 before 6.1.*, from 6.0.0 before 6.0.*, from 5.3.0 before 5.3.*.	N/A	More Details
CVE-2026-30802	Out-of-bounds Read vulnerability in RTI Connext Micro (Core Libraries) allows Overread Buffers.This issue affects Connext Micro: from 4.0.0 before 4.3.0.	N/A	More Details
CVE-2026-54310	n8n is an open source workflow automation platform. Prior to 2.25.7 and 2.26.2, an authenticated user with permission to create or modify workflows could supply a crafted parameters to the TimescaleDB and/or legacy Postgres v1 node's allowing arbitrary SQL to be injected and executed against the connected database within the privileges of the configured database account. This vulnerability is fixed in 2.25.7 and 2.26.2.	N/A	More Details
CVE-2026-12390	In AzeoTech DAQFactory versions 21.1 and prior, a Type Confusion vulnerability can be exploited by an attacker using specially crafted .ctl files which can result in code execution.	N/A	More Details
CVE-2026-30803	Integer Underflow (Wrap or Wraparound) vulnerability in RTI Connext Micro (Core Libraries) allows Overread Buffers.This issue affects Connext Micro: from 4.0.0 before 4.3.0.	N/A	More Details
CVE-	A flaw in Node.js HTTP/2 server API can cause servers to keep accepting data even after sending		

2026-48937	a `GOAWAY` frame. This vulnerability affects two supported release lines: **Node.js 22** and **Node.js 24**.	N/A	More Details
CVE-2026-54314	n8n is an open source workflow automation platform. Prior to 2.24.0, the Compression node's Decompress operation expanded attacker-controlled archives into memory without enforcing limits on decompressed output size. An unauthenticated attacker could send a small compressed archive to a public webhook workflow using this node, causing the n8n process to terminate due to memory exhaustion and disrupting all workflows in the same instance. This vulnerability is fixed in 2.24.0.	N/A	More Details
CVE-2026-54313	n8n is an open source workflow automation platform. Prior to 2.24.0, an authenticated user with workflow edit access could supply a malicious filter value in the MongoDB node's Find And Replace operation. The value was not validated before being passed to MongoDB as a query filter, allowing unintended documents to be matched and overwritten with attacker-controlled content. This vulnerability is fixed in 2.24.0.	N/A	More Details
CVE-2026-54312	n8n is an open source workflow automation platform. Prior to 2.24.0, an authenticated user with permission to create or modify workflows could achieve global prototype pollution via the Microsoft SQL node by supplying a crafted value as the table parameter. This pollutes Object.prototype process-wide for the lifetime of the n8n server process, causing application-wide validation failures and rendering the n8n instance completely non-functional until restarted. This vulnerability is fixed in 2.24.0.	N/A	More Details
CVE-2026-54311	n8n is an open source workflow automation platform. Prior to 2.25.7 and 2.26.2, an authenticated user with permission to create or modify workflows could pollute the sandbox used by the Merge node's SQL Query mode. Because the sandbox context was cached and reused across all workflow executions on the instance, prototype mutations introduced by one user's workflow persist into subsequent Merge SQL executions belonging to other users or projects. This allowed a low-privileged attacker to intercept workflow data processed by other users on the same instance. This issue only affects multi-user n8n instances where more than one user has permission to create and execute workflows containing the Merge node in SQL Query mode. This vulnerability is fixed in 2.25.7 and 2.26.2.	N/A	More Details
CVE-2026-54533	vantage6 is an open-source infrastructure for privacy preserving analysis. Prior to version 5.0.0, malicious algorithms can potentially access other algorithms input and output files. Version 5.0.0 fixes the issue. As a workaround, verify and restrict the algorithm containers that are allowed to run on the node.	N/A	More Details
CVE-2025-15641	Netskope was notified about a potential gap in its Netskope Client for Windows systems where a malicious insider with administrative privileges can potentially tamper with the customer IOCTL by sending crafted IOCTL requests to the driver. A successful exploit can result in the bypassing of all anti-tampering protections for the NSClient.Affected Product(s) and Version(s) * Product Name: Netskope Client * Affected Platform: Windows * Affected Version: All version below R138	N/A	More Details
CVE-2025-15642	Netskope is notified about a potential gap in its Netskoped Client for Windows systems where a malicious insider with admin privileges can lead to bypassing the NSClient Tamper Protections due to weak Discretionary Access Control List (DACLs) on the service object and related registry keys,. * Product Name: Netskope Client * Affected Platform: Windows * Affected Version: All version below R138	N/A	More Details
CVE-2026-11857	Quanos SCHEMA ST4 on-premises contains a local privilege escalation vulnerability in the Client Update Service due to insecure deserialization in the .NET Remoting service. The service is configured with TypeFilterLevel.Full and is bound to local interfaces only through named pipes. A local authenticated attacker can connect to the local named pipe, obtain the .NET Remoting endpoint, and send specially crafted serialized objects. Successful exploitation results in arbitrary code execution in the context of the update process with NT AUTHORITY\SYSTEM privileges. Network-only exploitation is not possible and local host access with an authenticated user session is required.	N/A	More Details
CVE-2026-10836	Improper handling of HTTP headers that allows a remote attacker to manipulate the value of the Host header using specially crafted requests. A successful exploit could result in the generation of manipulated links or responses, potentially leading to limited information disclosure or compromising the integrity of dependent services.	N/A	More Details
	Incorrect default permissions in ArubaSign, affecting versions prior to v4.6.6. The vulnerability is		

CVE-2026-12602	caused by the assignment of inappropriate permissions during the software's default installation, whereby the main executable and other programme files located in C:\Program Files have excessive permissions for the 'Everyone' group. This could allow an unprivileged user to replace the main executable and/or its components with a malicious file, thereby enabling the execution of arbitrary code. In the worst-case scenario, if the malicious code is executed with elevated privileges (such as those of Administrator or SYSTEM), the attacker could escalate privileges and gain full control of the system, compromising both security and data integrity.	N/A	More Details
CVE-2026-10837	Open redirection vulnerability due to insufficient validation of the X-Forwarded-Host HTTP header. An attacker could create manipulated links that, when opened by a victim, cause the victim to be redirected to domains controlled by the attacker, enabling phishing or deception attacks with limited impact on confidentiality and integrity.	N/A	More Details
CVE-2026-10720	Canonical MicroCeph versions from the squid and tentacle track are vulnerable to a path traversal issue in the remote-import API. Holders of a trusted cluster mTLS certificate (such as enrolled cluster members) or join token can manipulate files in an imported remote cluster within the /var/snap/microceph confinement. This would allow daemon disruption and pollution of the cluster state.	N/A	More Details
CVE-2026-54281	Nest is a framework for building scalable Node.js server-side applications. Prior to 11.1.24, an authentication bypass vulnerability exists in @nestjs/platform-fastify. When middleware is registered through NestJS's MiddlewareConsumer.forRoutes() API on the Fastify adapter, an unauthenticated client can bypass the Nest middleware registered for that route by simply appending a trailing slash (/) to the request URL. This bypass works on the default Fastify adapter configuration. This vulnerability is fixed in 11.1.24.	N/A	More Details
CVE-2026-10839	Open redirection vulnerability in the authentication system allows an attacker to use manipulated values in the X-Forwarded-Host header to alter the URLs generated by the application. A successful exploit could redirect authenticated users to malicious sites following login procedures or interaction with the interface, resulting in limited impact on confidentiality and integrity.	N/A	More Details
CVE-2026-11752	A vulnerability has been identified in armeria-xds versions 1.38.0 through 1.39.0, where DataSourceStream in the xDS module can resolve control-plane-supplied filenames and environment variables without restriction, allowing a compromised or semi-trusted xDS control plane to read arbitrary local files and environment variables on the xDS client host.	N/A	More Details
CVE-2026-11858	Quanos SCHEMA ST4 on-premises contains a local privilege escalation vulnerability in the Client Update Service. The update service runs as NT AUTHORITY\SYSTEM and exposes a .NET Remoting interface over a named pipe without sufficient access controls or authorization. A local authenticated low-privileged user can connect to the interface and invoke privileged update methods such as Update(). This allows arbitrary file write and delete operations with SYSTEM privileges and can be used to achieve local privilege escalation.	N/A	More Details
CVE-2026-8806	Expected Behavior Violation vulnerability in Mitsubishi Electric MELSEC iQ-F Series FX5-ENET/IP Ethernet Module FX5-ENET/IP all versions allows a remote attacker to cause a denial-of-service (DoS) condition in the affected product by continuously sending a large number of communication packets to the Ethernet port of the product in a short period of time, increasing the processing load of the product, preventing the internal anomaly-detection processing from being performed, and causing the communication function to stop.	N/A	More Details
CVE-2026-12888	An HTML injection vulnerability exists in the Google Chat webhook notification sent by Thinkst Applied Research Canarytokens, enabling Interface Manipulation in Google Chat. An attacker can insert limited HTML content including links. This issue affects Canarytokens: from Docker tag sha-4aef1db90 before sha-8ab4dccd, from Git commit 4aef1db90 before 8ab4dccd.	N/A	More Details
CVE-2026-12199	A vulnerability in `nltk.app.wordnet_app` up to version 3.9.3 allows unauthenticated remote shutdown of the local WordNet Browser HTTP server when started in its default mode. The server listens on all interfaces and processes a specific unauthenticated GET request (`/SHUTDOWN%20THE%20SERVER`) to terminate the process immediately via `os._exit(0)`. This results in a denial of service, impacting service availability. The issue arises due to insufficient authentication and protection mechanisms for critical server functions.	N/A	More Details
	DevGuard provides vulnerability management for the full software supply chain. Prior to 1.4.2, on a DevGuard API instance with one or more public assets, any authenticated user — including users from a different organization with no membership or role in the affected org/project — can		

CVE-2026-48089	create, update, reapply, and delete VEX rules on those public assets. The same flaw affects the other vulnerability-triage write endpoints exposed under a public asset, including VEX rule create / update / reapply / delete; dependency-vuln event creation (accept / reject / mitigate decisions), batch event creation, vuln sync, and mitigation; license risk creation; external reference writes; and/or artifact creation and license refresh. The attacker needs a valid account on the instance, but no membership in the victim organization, project, or asset is required. Version `v1.4.2`contains a patch. As a workaround, make affected assets non-public. In the asset settings, switch visibility from public to private. This removes the public-read exemption in the access-control middleware and restores correct authorization on all write endpoints for that asset. Downstream consumers that previously relied on the public `vex.json` / `sbom.json` endpoints will need to be granted explicit access or must receive an exported file version until the patched release is deployed.	N/A	More Details
CVE-2026-48715	radvd is a router advertisement daemon for IPv6. Prior to version 2.21, the `radvdump` utility shipped with radvd contains a stack buffer overflow in the Route Information option parser. When processing a crafted ICMPv6 Router Advertisement, `print_ff()` copies up to 2032 bytes from attacker-controlled packet data into a 16-byte `struct in6_addr` on the stack, overflowing by up to 2016 bytes. Note that the main `radvd` daemon is not affected by the vulnerability. Version 2.21 patches the issue.	N/A	More Details
CVE-2026-10741	Sonatype Nexus Repository Manager before 3.93.0 contains an authorization vulnerability in the proxy repository configuration that allows a delegated repository administrator to disclose stored upstream proxy credentials.	N/A	More Details
CVE-2026-56425	The Azure Active Directory (AAD) authentication implementation contained multiple weaknesses in its OAuth 2.0 authorization flow that could allow attackers to bypass important security guarantees provided by the protocol. The application used the PHP session identifier (session_id()) as the OAuth state parameter. Because session identifiers are long-lived authentication credentials, exposing them in OAuth redirect URLs could leak valid session tokens through browser history, HTTP Referer headers, reverse proxies, access logs, or third-party infrastructure involved in the authentication flow. If obtained by an attacker, the leaked session identifier could potentially be used for session hijacking. Additionally, the implementation did not regenerate the session identifier after successful authentication, leaving authenticated sessions susceptible to session fixation attacks where an attacker forces a victim to use a known session identifier before login and later reuses that identifier after authentication. The OAuth state value was also not implemented as a dedicated, single-use nonce. This weakened CSRF protections and increased the risk of replay attacks against the OAuth callback process. The authentication flow further failed to enforce HTTPS for the configured OAuth redirect URI. If a non-HTTPS redirect URI was used, OAuth authorization codes and access tokens could traverse the network in plaintext, exposing sensitive credentials to network attackers. Finally, OAuth error responses containing attacker-controlled GET parameters were logged verbatim. An attacker could inject control characters or crafted log content, leading to log forging, log injection, or corruption of audit records. The fix introduces: * A dedicated cryptographically random OAuth state value. * Single-use state validation and invalidation. * Constant-time state comparison using hash_equals(). * Session identifier rotation after successful authentication. * Enforcement of HTTPS-only redirect URIs. * Sanitized and length-limited logging of OAuth error parameters. AAD Authentication Plugin (OAuth 2.0 / Azure Active Directory integration)	N/A	More Details
CVE-2026-5667	Use of Hard-coded Credentials vulnerability in Mitsubishi Electric Room Air Conditioners (for Japan and outside Japan); Wireless LAN Adapters for Room Air Conditioners (for Japan and outside Japan); Wireless LAN Adapters for Packaged Air Conditioners (for Japan and outside Japan); Refrigerators (for Japan); Heat Pump Water Heaters / HEMS-Compatible Adapters / Wireless LAN Adapters (for Japan); Bathroom Dryer / Heater / Ventilation Systems (for Japan); Adapters for Airflow Ventilation Systems, Heat Pump Chilled / Hot Water Systems, and Ventilation / Air-Conditioning System Air Resorts (for Japan); Lossnay Central Ventilation Systems (for Japan); Smart Switches for Ventilation Fans and Lossnay (for Japan); IH Cooking Heaters (for Japan); and Rice Cookers (for Japan) allows an attacker within Wi-Fi radio range of an affected product to access the affected product using a hard-coded SSID and password, thereby obtaining device data such as operation status, room set temperature, and room temperature; changing the air-conditioner or Wi-Fi settings; or causing Wi-Fi communication to enter a denial-of-service (DoS) condition.	N/A	More Details
CVE-2026-	In Package Manager, there is a possible device lock controller bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution	N/A	More Details

0092	privileges needed. User interaction is not needed for exploitation.		
CVE-2026-8805	Integer Overflow or Wraparound vulnerability in the EtherNet/IP function of Mitsubishi Electric MELSEC iQ-F Series FX5-EIP EtherNet/IP module FX5-EIP versions 1.000 and prior allows a remote attacker to cause a denial-of-service (DoS) condition in the affected product by rapidly establishing a large number of TCP connections to it, resulting in an inconsistency in the product's internal connection management process and triggering improper memory access.	N/A	More Details
CVE-2026-45696	OpenEXR is the reference implementation and specification for the EXR image format, widely used in the motion picture industry. In versions 3.4.0 through 3.4.11, the HTJ2K (High-Throughput JPEG 2000) decoder, ht_undo_impl() in OpenEXRCore is vulnerable to a heap-buffer-overflow READ. The ht_undo_imp function copies decoded pixels out of a per-line OpenJPH buffer using the EXR channel's declared width as the iteration count. The codestream embedded in the EXR chunk can declare different (smaller) tile/line dimensions than the EXR header advertises, but ht_undo_impl() does not validate this — it pulls width 32-bit samples from cur_line->i32[] without checking the OpenJPH line buffer's actual length. A crafted EXR file produces a 4-byte heap-buffer-overflow READ immediately after a buffer allocated by ojph::local::codestream::finalize_alloc(). The bug is reachable through the standard scanline-decode entry point used by every consumer of exr_decoding_run/Imf::checkOpenEXRFile, including thumbnailers, asset pipelines, and the exrcheck utility — i.e. any application that opens untrusted EXR files. The result is a deterministic crash (DoS) and potential adjacent-heap leak. This issue has been fixed in version 3.4.12.	N/A	More Details
CVE-2026-12863	An unvalidated redirect was contained in Venueless' social login functionality and could be exploited for phishing using trusted domains.	N/A	More Details
CVE-2026-54445	vantage6 is an open-source infrastructure for privacy preserving analysis. Versions prior to 5.0.0 provide an initial user with username `root` and password `root`. This is not ideal because attackers know that almost all vantage6 servers have a user with username `root` that probably has admin rights, and the initial password is very weak and it is possible that administrators forget to reset it. Version 5.0.0 fixes the issue. As a workaround, it is possible to delete the `root` user after it has been used to create other users.	N/A	More Details
CVE-2026-49248	OneDev is a Git server with CI/CD, kanban, and packages. In versions 15.0.6 and below, TarUtils.untar() creates symbolic links verbatim from TAR entry getLinkName() without validating whether the target is an absolute path. A subsequent file entry in the same archive traverses the symlink, writing to arbitrary server-side locations. This is exploitable by any authenticated user with CI Job write access — no admin interaction required. This is an incomplete fix bypass of CVE-2021-21251 (GHSA-2w6j-wc8c-9mq2): that patch blocked .. path segments but did not address absolute symlink targets. This issue has been fixed in version 15.0.7.	N/A	More Details
CVE-2026-53676	ThingsBoard contains a prototype pollution vulnerability which may lead to arbitrary code execution within a sandboxed context by a user who can log in to the affected product with the tenant administrator privilege (TENANT_ADMIN).	N/A	More Details
CVE-2026-12862	Untrusted user data was passed verbatim to Excel exports for administrators. This allowed formula injection which can be used to compromise the environment of the user loading the file or other data in the file.	N/A	More Details
CVE-2026-11833	Overview: A vulnerability has been found in FAST/TOOLS and CI Server. The web server may return a response containing the CI Server setting information. 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 CI Server (All packages) R1.01 to R1.04	N/A	More Details
CVE-2026-8100	Impact A security issue has been identified in Chef 360 that could allow unauthorized access to protected API endpoints under specific conditions. This issue is due to improper handling of URL-encoded paths during request processing. In certain scenarios, an authenticated request may bypass standard access controls gaining additional privileges, potentially allowing access to API endpoints that are intended to be restricted to higher-permissioned roles. The impact is limited to environments where the affected request patterns can be triggered and depends on specific deployment configuration and access controls in place. Resolution The issue has been addressed through product updates that improve request validation and enforce strict path normalization	N/A	More Details

	before authorization checks. Customers are advised to update to the latest available version containing the fix, version 1.7.1 or later.		
CVE-2026-8668	A static credential embedded in Chef 360 prior to v1.7.0 permitted unauthenticated access to internal message queues. Queue messages contained tenant-specific identifiers. The credential has been rotated and replaced with per-tenant access in subsequent versions, eliminating this access method entirely.	N/A	More Details
CVE-2026-56422	Multiple MISP core controllers and model capture paths accepted client-controlled request fields such as primary keys (id) and ownership/scope foreign keys (event_id, org_id, user_id, sharing_group_id, galaxy_cluster_uuid, organisation_uuid, and related nested object identifiers) without consistently stripping, pinning, or revalidating them against the server-authorized object. In affected paths, an authenticated user with access to one authorized object could submit crafted REST or form payloads that caused MISP to save data against a different object than the one checked by the authorization logic. Depending on the endpoint, this could allow object overwrite, object re-parenting, ownership transfer, unauthorized sharing-group scoping, event/object injection, proposal retargeting, or stored attacker-controlled content appearing in another user’s context. The fixes harden affected create/edit/import flows by stripping client-supplied primary keys on create-only saves, re-pinning route- or database-authorized identifiers before save operations, validating effective sharing-group scope, and adding field whitelists where ownership fields must never be editable. The initial broad fix also added a central CRUDComponent::edit() primary-key re-pin so payload-supplied IDs cannot redirect saves away from the already-authorized row. GitHub’s patch for 7acf8220c describes this central issue as CRUDComponent::edit() copying supplied fields, including a payload primary key, onto the loaded record, allowing CakePHP save() to update an arbitrary row unless the loaded ID is re-pinned.	N/A	More Details
CVE-2026-9375	urllib3 version 2.6.3 is vulnerable to a decompression bomb bypass in its streaming API (`preload_content=False`) when using Brotli support. The issue arises due to three independent code paths in `response.py` that bypass the `max_length` protection introduced in version 2.6.0 to mitigate CVE-2025-66471. Specifically, negative `max_length` values can be produced due to buffer arithmetic in `read()`, `flush_decoder` unconditionally overrides `max_length` to `-1`, and `_flush_decoder()` passes no limit at all, defaulting to unlimited decompression. This allows a malicious HTTP server to trigger an out-of-memory (OOM) condition by decompressing large payloads into memory, leading to a denial of service (DoS). The vulnerability affects urllib3 2.6.3 and Brotli 1.2.0 and impacts applications and libraries using `requests` or `urllib3` to stream content from untrusted sources.	N/A	More Details
CVE-2026-54235	vLLM is an inference and serving engine for large language models (LLMs). Prior to 0.23.1rc0, ll temperature validation gates use comparison operators (<, >), which silently evaluate to False for NaN and for positive Infinity in Python's IEEE 754 float semantics. Both values pass every guard and propagate to GPU sampling kernels, where they produce undefined behavior or CUDA errors that can crash the inference worker. This vulnerability is fixed in 0.23.1rc0.	N/A	More Details
CVE-2026-10746	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2026-9591	Cross-site request forgery (CSRF) in NewsItemApiController in SimplCommerce prior to commit 6233d73e allows an unauthenticated remote attacker to create or modify news items as an administrator via a crafted form submitted to `/api/news-items`, due to missing anti-CSRF protection.	N/A	More Details
CVE-2026-53923	vLLM is an inference and serving engine for large language models (LLMs). From 0.5.5 until 0.23.1rc0, integer truncation of tensor dimensions in vLLM's GGUF dequantize kernels (csrc/quantization/gguf/gguf_kernel.cu) causes partial tensor processing. The output tensor is allocated at full size via torch::empty (uninitialized memory), but the dequantize CUDA kernel processes only a truncated number of elements. The unfilled portion of the output tensor retains whatever was previously in GPU memory. In multi-tenant inference deployments, this residual GPU memory may contain tensor data from other users' inference requests, constituting information disclosure. This vulnerability is fixed in 0.23.1rc0.	N/A	More Details
CVE-2026-6716	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details

CVE-2026-52909	In the Linux kernel, the following vulnerability has been resolved: ip6_vti: set netns_immutable on the fallback device. john1988 and Noam Rathaus reported that vti6_init_net() does not set the netns_immutable flag on the per-netns fallback tunnel device (ip6_vti0). Other similar tunnel drivers (like ip6_tunnel, sit, ip6_gre, and ip_tunnel) correctly set this flag during their fallback device initialization to prevent them from being moved to another network namespace.	N/A	More Details
CVE-2026-52908	In the Linux kernel, the following vulnerability has been resolved: RDMA: During rereg_mr ensure that REREG_ACCESS is compatible If IB_MR_REREG_ACCESS changes from RO to RW then the umem has to be re-evaluated to ensure it is properly pinned as RW. Since the umem is hidden inside each driver's mr struct add a ib_umem_check_rereg() function that each driver has to call before processing IB_MR_REREG_ACCESS. mlx4 has to retain its duplicate ib_access_writable check because it implements IB_MR_REREG_ACCESS | IB_MR_REREG_TRANS by changing both items in place sequentially while the MR is live, so it will continue to not support this combination.	N/A	More Details
CVE-2026-11975	Stored cross-site scripting (XSS) in NewsItemApiController In SimplCommerce prior to commit 6142d3b5 allows an authenticated administrator to execute arbitrary JavaScript via the ShortContent and FullContent fields, which are stored without HTML sanitization and rendered unencoded via @Html.Raw()	N/A	More Details