الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

تمت مشاركة هذه المعلومة بإشارة مشاركة ***أبيض*** حيث يسمح بتبادلها أو نشرها من خلال القنوات العامة.

في ضوء دور الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء السيبراني الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للثغرات المسجلة من قبل the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) للأسبوع من 5 أبريل إلى 11 أبريل. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

- **عالي جدًا: النتيجة الأساسية لـCVSS 9.0-10.0**
- **عالي: النتيجة الأساسية لـCVSS 7.0-8.9**
- **متوسط: النتيجة الأساسية لـCVSS 4.0-6.9**
- **منخفض: النتيجة الأساسية لـ CVSS 0.0-3.9**

Please note that this notification/advisory has been tagged as TLP ***WHITE*** where information can be shared or published on any public forums.

As part of NCA duties to help securing the cyberspace and protecting national interests, NCA provides the weekly summary of published vulnerabilities by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) for the week from 5th of April to 11th of April. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

- **Critical: CVSS base score of 9.0-10.0**
- **High: CVSS base score of 7.0-8.9**
- **Medium: CVSS base score 4.0-6.9**
- **Low: CVSS base score 0.0-3.9**

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score
CVE-2025-54328	samsung - exynos_980_firmware	An issue was discovered in SMS in Samsung Mobile Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 1280, 2200, 1330, 1380, 1480, 2400, 1580, 2500, 9110, W920, W930, W1000, Modem 5123, Modem 5300, and Modem 5400. A Stack-based Buffer Overflow occurs while parsing SMS RP-DATA messages.	2026-04-06	10
CVE-2026-5731	mozilla - multiple products	Memory safety bugs present in Firefox ESR 115.34.0, Firefox ESR 140.9.0, Thunderbird ESR 140.9.0, Firefox 149.0.1 and Thunderbird 149.0.1. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability was fixed in Firefox 149.0.2, Firefox ESR 115.34.1, Firefox ESR 140.9.1, Thunderbird 149.0.2, and Thunderbird 140.9.1.	2026-04-07	9.8
CVE-2026-5734	mozilla - multiple products	Memory safety bugs present in Firefox ESR 140.9.0, Thunderbird ESR 140.9.0, Firefox 149.0.1 and Thunderbird 149.0.1. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability was fixed in Firefox 149.0.2, Firefox ESR 140.9.1, Thunderbird 149.0.2, and Thunderbird 140.9.1.	2026-04-07	9.8
CVE-2026-5735	mozilla - multiple products	Memory safety bugs present in Firefox 149.0.1 and Thunderbird 149.0.1. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability was fixed in Firefox 149.0.2 and Thunderbird 149.0.2.	2026-04-07	9.8
CVE-2025-52909	samsung - exynos_1280_firmware	An issue was discovered in the Wi-Fi driver in Samsung Mobile Processor and Wearable Processor Exynos 980, 850, 1280, 1330, 1380, 1480, 1580, W920, W930, and W1000. Incorrect Handling of the NL80211 vendor command leads to a buffer overflow via a certain ioctl message, issue 2 of 2.	2026-04-07	9.8
CVE-2025-62818	samsung - exynos_990_firmware	An issue was discovered in Samsung Mobile Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 1280, 2200, 1330, 1380, 1480, 2400, 1580, 2500, 9110, W920, W930, W1000, Modem 5123, Modem 5300, and Modem 5400. An out-of-bounds write occurs due to a mismatch between the TP-UDHI and UDL values when processing an SMS TP-UD packet.	2026-04-07	9.8
CVE-2025-52908	samsung - exynos_1280_firmware	An issue was discovered in the Wi-Fi driver in Samsung Mobile Processor and Wearable Processor Exynos 980, 850, 1280, 1330, 1380, 1480, 1580, W920, W930, and W1000. Incorrect Handling of the NL80211 vendor command leads to a buffer overflow via a certain ioctl message, issue 1 of 2.	2026-04-07	9.8
CVE-2026-4631	red hat - multiple products	Cockpit's remote login feature passes user-supplied hostnames and usernames from the web interface to the SSH client without validation or sanitization. An attacker with network access to the Cockpit web service can craft a single HTTP request to the login endpoint that injects malicious SSH options or shell commands, achieving code execution on the Cockpit host without valid credentials. The injection occurs during the authentication flow before any credential verification takes place, meaning no login is required to exploit the vulnerability.	2026-04-07	9.8
CVE-2026-5902	google - chrome	Race in Media in Google Chrome on Android prior to 147.0.7727.55 allowed a remote attacker who had compromised the renderer process to corrupt media stream metadata via a crafted HTML page. (Chromium security severity: Low)	2026-04-08	9.8

CVE-2026-5874	google - chrome	Use after free in PrivateAI in Google Chrome prior to 147.0.7727.55 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-04-08	9.6
CVE-2026-1346	ibm - multiple products	IBM Verify Identity Access Container 11.0 through 11.0.2 and IBM Security Verify Access Container 10.0 through 10.0.9.1 and IBM Verify Identity Access 11.0 through 11.0.2 and IBM Security Verify Access 10.0 through 10.0.9.1 could allow a locally authenticated user to escalate their privileges to root due to execution with unnecessary privileges than required.	2026-04-08	9.3
CVE-2025-58349	samsung - exynos_990_firmware	An issue was discovered in L2 in Samsung Mobile Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 1280, 2200, 1330, 1380, 1480, 2400, 1580, 2500, 9110, W920, W930, W1000, Modem 5123, Modem 5300, and Modem 5400. Incorrect handling of LTE MAC packets containing many MAC Control Elements (CEs) leads to baseband crashes.	2026-04-06	9.1
CVE-2026-28386	openssl - OpenSSL	Issue summary: Applications using AES-CFB128 encryption or decryption on systems with AVX-512 and VAES support can trigger an out-of-bounds read of up to 15 bytes when processing partial cipher blocks. Impact summary: This out-of-bounds read may trigger a crash which leads to Denial of Service for an application if the input buffer ends at a memory page boundary and the following page is unmapped. There is no information disclosure as the over-read bytes are not written to output. The vulnerable code path is only reached when processing partial blocks (when a previous call left an incomplete block and the current call provides fewer bytes than needed to complete it). Additionally, the input buffer must be positioned at a page boundary with the following page unmapped. CFB mode is not used in TLS/DTLS protocols, which use CBC, GCM, CCM, or ChaCha20-Poly1305 instead. For these reasons the issue was assessed as Low severity according to our Security Policy. Only x86-64 systems with AVX-512 and VAES instruction support are affected. Other architectures and systems without VAES support use different code paths that are not affected. OpenSSL FIPS module in 3.6 version is affected by this issue.	2026-04-07	9.1
CVE-2025-57735	apache - airflow	When user logged out, the JWT token the user had authtenticated with was not invalidated, which could lead to reuse of that token in case it was intercepted. In Airflow 3.2 we implemented the mechanism that implements token invalidation at logout. Users who are concerned about the logout scenario and possibility of intercepting the tokens, should upgrade to Airflow 3.2+ Users are recommended to upgrade to version 3.2.0, which fixes this issue.	2026-04-09	9.1
CVE-2026-29145	apache - multiple products	CLIENT_CERT authentication does not fail as expected for some scenarios when soft fail is disabled vulnerability in Apache Tomcat, Apache Tomcat Native. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.18, from 10.1.0-M7 through 10.1.52, from 9.0.83 through 9.0.115; Apache Tomcat Native: from 1.1.23 through 1.1.34, from 1.2.0 through 1.2.39, from 1.3.0 through 1.3.6, from 2.0.0 through 2.0.13. Users are recommended to upgrade to version Tomcat Native 1.3.7 or 2.0.14 and Tomcat 11.0.20, 10.1.53 and 9.0.116, which fix the issue.	2026-04-09	9.1
CVE-2025-47392	qualcomm - 5g_fixed_wireless_access_platform_firmware	Memory corruption when decoding corrupted satellite data files with invalid signature offsets.	2026-04-06	8.8
CVE-2026-34197	apache - multiple products	Improper Input Validation, Improper Control of Generation of Code ('Code Injection') vulnerability in Apache ActiveMQ Broker, Apache ActiveMQ. Apache ActiveMQ Classic exposes the Jolokia JMX-HTTP bridge at /api/jolokia/ on the web console. The default Jolokia access policy permits exec operations on all ActiveMQ MBeans (org.apache.activemq:*), including BrokerService.addNetworkConnector(String) and BrokerService.addConnector(String). An authenticated attacker can invoke these operations with a crafted discovery URI that triggers the VM transport's brokerConfig parameter to load a remote Spring XML application context using ResourceXmlApplicationContext. Because Spring's ResourceXmlApplicationContext instantiates all singleton beans before the BrokerService validates the configuration, arbitrary code execution occurs on the broker's JVM through bean factory methods such as Runtime.exec().	2026-04-07	8.8

		This issue affects Apache ActiveMQ Broker: before 5.19.4, from 6.0.0 before 6.2.3; Apache ActiveMQ All: before 5.19.4, from 6.0.0 before 6.2.3; Apache ActiveMQ: before 5.19.4, from 6.0.0 before 6.2.3. Users are recommended to upgrade to version 5.19.4 or 6.2.3, which fixes the issue		
CVE-2026-5732	mozilla - multiple products	Incorrect boundary conditions, integer overflow in the Graphics: Text component. This vulnerability was fixed in Firefox 149.0.2, Firefox ESR 140.9.1, Thunderbird 149.0.2, and Thunderbird 140.9.1.	2026-04-07	8.8
CVE-2026-5733	mozilla - firefox	Incorrect boundary conditions in the Graphics: WebGPU component. This vulnerability was fixed in Firefox 149.0.2 and Thunderbird 149.0.2.	2026-04-07	8.8
CVE-2026-35517	pi-hole - FTL	FTLDNS (pihole-FTL) provides an interactive API and also generates statistics for Pi-hole's Web interface. From 6.0 to before 6.6, the Pi-hole FTL engine contains a Remote Code Execution (RCE) vulnerability in the upstream DNS servers configuration parameter (dns.upstreams). This vulnerability allows an authenticated attacker to inject arbitrary dnsmasq configuration directives through newline characters, ultimately achieving command execution on the underlying system. This vulnerability is fixed in 6.6.	2026-04-07	8.8
CVE-2026-35518	pi-hole - FTL	FTLDNS (pihole-FTL) provides an interactive API and also generates statistics for Pi-hole's Web interface. From 6.0 to before 6.6, the Pi-hole FTL engine contains a Remote Code Execution (RCE) vulnerability in the DNS CNAME records configuration parameter (dns.cnameRecords). This vulnerability allows an authenticated attacker to inject arbitrary dnsmasq configuration directives through newline characters, ultimately achieving command execution on the underlying system. This vulnerability is fixed in 6.6.	2026-04-07	8.8
CVE-2026-35519	pi-hole - FTL	FTLDNS (pihole-FTL) provides an interactive API and also generates statistics for Pi-hole's Web interface. From 6.0 to before 6.6, the Pi-hole FTL engine contains a Remote Code Execution (RCE) vulnerability in the DNS host record configuration parameter (dns.hostRecord). This vulnerability allows an authenticated attacker to inject arbitrary dnsmasq configuration directives through newline characters, ultimately achieving command execution on the underlying system. This vulnerability is fixed in 6.6.	2026-04-07	8.8
CVE-2026-35520	pi-hole - FTL	FTLDNS (pihole-FTL) provides an interactive API and also generates statistics for Pi-hole's Web interface. From 6.0 to before 6.6, the Pi-hole FTL engine contains a Remote Code Execution (RCE) vulnerability in the DHCP lease time configuration parameter (dhcp.leaseTime). This vulnerability allows an authenticated attacker to inject arbitrary dnsmasq configuration directives through newline characters, ultimately achieving command execution on the underlying system. This vulnerability is fixed in 6.6.	2026-04-07	8.8
CVE-2026-35521	pi-hole - FTL	FTLDNS (pihole-FTL) provides an interactive API and also generates statistics for Pi-hole's Web interface. From 6.0 to before 6.6, the Pi-hole FTL engine contains a Remote Code Execution (RCE) vulnerability in the DHCP hosts configuration parameter (dhcp.hosts). This vulnerability allows an authenticated attacker to inject arbitrary dnsmasq configuration directives through newline characters, ultimately achieving command execution on the underlying system. This vulnerability is fixed in 6.6.	2026-04-07	8.8
CVE-2026-27314	apache - cassandra	Privilege escalation in Apache Cassandra 5.0 on an mTLS environment using MutualTlsAuthenticator allows a user with only CREATE permission to associate their own certificate identity with an arbitrary role, including a superuser role, and authenticate as that role via ADD IDENTITY. Users are recommended to upgrade to version 5.0.7+, which fixes this issue.	2026-04-07	8.8
CVE-2026-5858	google - chrome	Heap buffer overflow in WebML in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: Critical)	2026-04-08	8.8
CVE-2026-5859	google - chrome	Integer overflow in WebML in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical)	2026-04-08	8.8
CVE-2026-5860	google - chrome	Use after free in WebRTC in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-04-08	8.8
CVE-2026-5861	google - chrome	Use after free in V8 in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-04-08	8.8
CVE-2026-5862	google - chrome	Inappropriate implementation in V8 in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-04-08	8.8
CVE-2026-5863	google - chrome	Inappropriate implementation in V8 in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-04-08	8.8
CVE-2026-5865	google - chrome	Type Confusion in V8 in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-04-08	8.8

CVE-2026-5866	google - chrome	Use after free in Media in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-04-08	8.8
CVE-2026-5868	google - chrome	Heap buffer overflow in ANGLE in Google Chrome on Mac prior to 147.0.7727.55 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-04-08	8.8
CVE-2026-5870	google - chrome	Integer overflow in Skia in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-04-08	8.8
CVE-2026-5871	google - chrome	Type Confusion in V8 in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-04-08	8.8
CVE-2026-5872	google - chrome	Use after free in Blink in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-04-08	8.8
CVE-2026-5873	google - chrome	Out of bounds read and write in V8 in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-04-08	8.8
CVE-2026-5877	google - chrome	Use after free in Navigation in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	2026-04-08	8.8
CVE-2026-5879	google - chrome	Insufficient validation of untrusted input in ANGLE in Google Chrome on Mac prior to 147.0.7727.55 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	2026-04-08	8.8
CVE-2026-5883	google - chrome	Use after free in Media in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	2026-04-08	8.8
CVE-2026-5884	google - chrome	Insufficient validation of untrusted input in Media in Google Chrome prior to 147.0.7727.55 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: Medium)	2026-04-08	8.8
CVE-2026-5904	google - chrome	Use after free in V8 in Google Chrome prior to 147.0.7727.55 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: Low)	2026-04-08	8.8
CVE-2026-5908	google - chrome	Integer overflow in Media in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to potentially exploit heap corruption via a crafted video file. (Chromium security severity: Low)	2026-04-08	8.8
CVE-2026-5909	google - chrome	Integer overflow in Media in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to potentially exploit heap corruption via a crafted video file. (Chromium security severity: Low)	2026-04-08	8.8
CVE-2026-5910	google - chrome	Integer overflow in Media in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to potentially exploit heap corruption via a crafted video file. (Chromium security severity: Low)	2026-04-08	8.8
CVE-2026-5912	google - chrome	Integer overflow in WebRTC in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: Low)	2026-04-08	8.8
CVE-2026-5914	google - chrome	Type Confusion in CSS in Google Chrome prior to 147.0.7727.55 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: Low)	2026-04-08	8.8
CVE-2026-35554	apache software foundation - Apache Kafka Clients	A race condition in the Apache Kafka Java producer client's buffer pool management can cause messages to be silently delivered to incorrect topics. When a produce batch expires due to delivery.timeout.ms while a network request containing that batch is still in flight, the batch's ByteBuffer is prematurely deallocated and returned to the buffer pool. If a subsequent producer batch—potentially destined for a different topic—reuses this freed buffer before the original network request completes, the buffer contents may become corrupted. This can result in messages being delivered to unintended topics without any error being reported to the producer. Data Confidentiality: Messages intended for one topic may be delivered to a different topic, potentially exposing sensitive data to consumers who have access to the destination topic but not the intended source topic. Data Integrity: Consumers on the receiving topic may encounter unexpected or incompatible messages, leading to deserialization failures, processing errors, and corrupted downstream data. This issue affects Apache Kafka versions ≤ 3.9.1, ≤ 4.0.1, and ≤ 4.1.1. Kafka users are advised to upgrade to 3.9.2, 4.0.2, 4.1.2, 4.2.0, or later to address this vulnerability.	2026-04-07	8.7

CVE-2026-33778	juniper - multiple products	An Improper Validation of Syntactic Correctness of Input vulnerability in the IPsec library used by kmd and iked of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a complete Denial-of-Service (DoS). If an affected device receives a specifically malformed first ISAKMP packet from the initiator, the kmd/iked process will crash and restart, which momentarily prevents new security associations (SAs) for from being established. Repeated exploitation of this vulnerability causes a complete inability to establish new VPN connections. This issue affects Junos OS on SRX Series and MX Series: * all versions before 22.4R3-S9, * 23.2 version before 23.2R2-S6, * 23.4 version before 23.4R2-S7, * 24.2 versions before 24.2R2-S4, * 24.4 versions before 24.4R2-S3, * 25.2 versions before 25.2R1-S2, 25.2R2.	2026-04-09	8.7
CVE-2026-33782	juniper - multiple products	A Missing Release of Memory after Effective Lifetime vulnerability in the DHCP daemon (jdhcpd) of Juniper Networks Junos OS on MX Series, allows an adjacent, unauthenticated attacker to cause a memory leak, that will eventually cause a complete Denial-of-Service (DoS). In a DHCPv6 over PPPoE, or DHCPv6 over VLAN with Active lease query or Bulk lease query scenario, every subscriber logout will leak a small amount of memory. When all available memory has been exhausted, jdhcpd will crash and restart which causes a complete service impact until the process has recovered. The memory usage of jdhcpd can be monitored with: user@host> show system processes extensive | match jdhcpd This issue affects Junos OS: * all versions before 22.4R3-S1, * 23.2 versions before 23.2R2, * 23.4 versions before 23.4R2.	2026-04-09	8.7
CVE-2026-33790	juniper - multiple products	An Improper Check for Unusual or Exceptional Conditions vulnerability in the flow daemon (flowd) of Juniper Networks Junos OS on SRX Series allows an attacker sending a specific, malformed ICMPv6 packet to cause the srxpfe process to crash and restart. Continued receipt and processing of these packets will repeatedly crash the srxpfe process and sustain the Denial of Service (DoS) condition. During NAT64 translation, receipt of a specific, malformed ICMPv6 packet destined to the device will cause the srxpfe process to crash and restart. This issue cannot be triggered using IPv4 nor other IPv6 traffic. This issue affects Junos OS on SRX Series: * all versions before 21.2R3-S10, * all versions of 21.3, * from 21.4 before 21.4R3-S12, * all versions of 22.1, * from 22.2 before 22.2R3-S8, * all versions of 22.4, * from 22.4 before 22.4R3-S9, * from 23.2 before 23.2R2-S6, * from 23.4 before 23.4R2-S7, * from 24.2 before 24.2R2-S3, * from 24.4 before 24.4R2-S3, * from 25.2 before 25.2R1-S2, 25.2R2.	2026-04-09	8.7
CVE-2026-34621	adobe - multiple products	Acrobat Reader versions 24.001.30356, 26.001.21367 and earlier are affected by an Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') 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.	2026-04-11	8.6

CVE-2026-1342	ibm - multiple products	IBM Verify Identity Access Container 11.0 through 11.0.2 and IBM Security Verify Access Container 10.0 through 10.0.9.1 and IBM Verify Identity Access 11.0 through 11.0.2 and IBM Security Verify Access 10.0 through 10.0.9.1 could allow a locally authenticated user to execute malicious scripts from outside of its control sphere.	2026-04-08	8.5
CVE-2026-30815	tp-link - archer_ax53_firmware	An OS command injection vulnerability in the OpenVPN module of TP-Link Archer AX53 v1.0 allows an authenticated adjacent attacker to execute system commands when a specially crafted configuration file is processed due to insufficient input validation. Successful exploitation may allow modification of configuration files, disclosure of sensitive information, or further compromise of device integrity. This issue affects AX53 v1.0: before 1.7.1 Build 20260213.	2026-04-08	8.5
CVE-2026-30818	tp-link - archer_ax53_firmware	An OS command injection vulnerability in the dnsmasq module of TP-Link Archer AX53 v1.0 allows an authenticated adjacent attacker to execute arbitrary code when a specially crafted configuration file is processed due to insufficient input validation. Successful exploitation may allow the attacker to modify device configuration, access sensitive information, or further compromise system integrity. This issue affects AX53 v1.0: before 1.7.1 Build 20260213.	2026-04-08	8.5
CVE-2026-33793	juniper - multiple products	An Execution with Unnecessary Privileges vulnerability in the User Interface (UI) of Juniper Networks Junos OS and Junos OS Evolved allows a local, low-privileged attacker to gain root privileges, thus compromising the system. When a configuration that allows unsigned Python op scripts is present on the device, a non-root user is able to execute malicious op scripts as a root-equivalent user, leading to privilege escalation. This issue affects Junos OS: * All versions before 22.4R3-S7, * from 23.2 before 23.2R2-S4, * from 23.4 before 23.4R2-S6, * from 24.2 before 24.2R1-S2, 24.2R2, * from 24.4 before 24.4R1-S2, 24.4R2; Junos OS Evolved: * All versions before 22.4R3-S7-EVO, * from 23.2 before 23.2R2-S4-EVO, * from 23.4 before 23.4R2-S6-EVO, * from 24.2 before 24.2R2-EVO, * from 24.4 before 24.4R1-S1-EVO, 24.4R2-EVO.	2026-04-09	8.5
CVE-2026-5483	red hat - multiple products	A flaw was found in odh-dashboard in Red Hat Openshift AI. This vulnerability in the `odh-dashboard` component of Red Hat OpenShift AI (RHOAI) allows for the disclosure of Kubernetes Service Account tokens through a NodeJS endpoint. This could enable an attacker to gain unauthorized access to Kubernetes resources.	2026-04-10	8.5
CVE-2026-4788	ibm - tivoli_netcool\/impact	IBM Tivoli Netcool Impact 7.1.0.0 through 7.1.0.37 stores sensitive information in log files that could be read by a local user.	2026-04-08	8.4
CVE-2026-33791	juniper - multiple products	An OS Command Injection vulnerability in the CLI processing of Juniper Networks Junos OS and Junos OS Evolved allows a local, high-privileged attacker executing specific, crafted CLI commands to inject arbitrary shell commands as root, leading to a complete compromise of the system. Certain 'set system' commands, when executed with crafted arguments, are not properly sanitized, allowing for arbitrary shell injection. These shell commands are executed as root, potentially allowing for complete control of the vulnerable system. This issue affects: Junos OS: * all versions before 22.4R3-S8, * from 23.2 before 23.2R2-S5, * from 23.4 before 23.4R2-S7, * from 24.2 before 24.2R2-S2, * from 24.4 before 24.4R2, * from 25.2 before 25.2R2;	2026-04-09	8.4

		Junos OS Evolved: * all versions before 22.4R3-S8-EVO, * from 23.2 before 23.2R2-S5-EVO, * from 23.4 before 23.4R2-S7-EVO, * from 24.2 before 24.2R2-S2-EVO, * from 24.4 before 24.4R2-EVO, * from 25.2 before 25.2R1-S1-EVO, 25.2R2-EVO.		
CVE-2026-33779	juniper - multiple products	An Improper Following of a Certificate's Chain of Trust vulnerability in J-Web of Juniper Networks Junos OS on SRX Series allows a PITM to intercept the communication of the device and get access to confidential information and potentially modify it. When an SRX device is provisioned to connect to Security Director (SD) cloud, it doesn't perform sufficient verification of the received server certificate. This allows a PITM to intercept the communication between the SRX and SD cloud and access credentials and other sensitive information. This issue affects Junos OS: * all versions before 22.4R3-S9, * 23.2 versions before 23.2R2-S6, * 23.4 versions before 23.4R2-S7, * 24.2 versions before 24.2R2-S3, * 24.4 versions before 24.4R2-S2, * 25.2 versions before 25.2R1-S2, 25.2R2.	2026-04-09	8.3
CVE-2026-4740	red hat - multiple products	A flaw was found in Open Cluster Management (OCM), the technology underlying Red Hat Advanced Cluster Management (ACM). Improper validation of Kubernetes client certificate renewal allows a managed cluster administrator to forge a client certificate that can be approved by the OCM controller. This enables cross-cluster privilege escalation and may allow an attacker to gain control over other managed clusters, including the hub cluster.	2026-04-07	8.2
CVE-2026-5907	google - chrome	Insufficient data validation in Media in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to perform an out of bounds memory read via a crafted video file. (Chromium security severity: Low)	2026-04-08	8.1
CVE-2026-5913	google - chrome	Out of bounds read in Blink in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: Low)	2026-04-08	8.1
CVE-2026-5915	google - chrome	Insufficient validation of untrusted input in WebML in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: Low)	2026-04-08	8.1
CVE-2021-47961	synology - Synology SSL VPN Client	A plaintext storage of a password vulnerability in Synology SSL VPN Client before 1.4.5-0684 allows remote attackers to access or influence the user's PIN code due to insecure storage. This may lead to unauthorized VPN configuration and potential interception of subsequent VPN traffic when combined with user interaction.	2026-04-10	8.1
CVE-2025-47389	qualcomm - ar8035_firmware	Memory corruption when buffer copy operation fails due to integer overflow during attestation report generation.	2026-04-06	7.8
CVE-2025-47390	qualcomm - qcm5430_firmware	Memory corruption while preprocessing IOCTL request in JPEG driver.	2026-04-06	7.8
CVE-2025-47391	qualcomm - wcn3988_firmware	Memory corruption while processing a frame request from user.	2026-04-06	7.8
CVE-2026-21371	qualcomm - aqt1000_firmware	Memory Corruption when retrieving output buffer with insufficient size validation.	2026-04-06	7.8
CVE-2026-21372	qualcomm - cologne_firmware	Memory Corruption when sending IOCTL requests with invalid buffer sizes during memcpy operations.	2026-04-06	7.8
CVE-2026-21373	qualcomm - aqt1000_firmware	Memory Corruption when accessing an output buffer without validating its size during IOCTL processing.	2026-04-06	7.8
CVE-2026-21374	qualcomm - aqt1000_firmware	Memory Corruption when processing auxiliary sensor input/output control commands with insufficient buffer size validation.	2026-04-06	7.8
CVE-2026-21375	qualcomm - cologne_firmware	Memory Corruption when accessing an output buffer without validating its size during IOCTL processing.	2026-04-06	7.8

CVE-2026-21376	qualcomm - aqt1000_firmware	Memory Corruption when accessing an output buffer without validating its size during IOCTL processing in a camera sensor driver.	2026-04-06	7.8
CVE-2026-21378	qualcomm - fastconnect_6900_firmware	Memory Corruption when accessing an output buffer without validating its size during IOCTL processing in a camera sensor driver.	2026-04-06	7.8
CVE-2026-21380	qualcomm - cologne_firmware	Memory Corruption when using deprecated DMABUF IOCTL calls to manage video memory.	2026-04-06	7.8
CVE-2026-21382	qualcomm - cologne_firmware	Memory Corruption when handling power management requests with improperly sized input/output buffers.	2026-04-06	7.8
CVE-2025-14821	red hat - multiple products	A flaw was found in libssh. This vulnerability allows local man-in-the-middle attacks, security downgrades of SSH (Secure Shell) connections, and manipulation of trusted host information, posing a significant risk to the confidentiality, integrity, and availability of SSH communications via an insecure default configuration on Windows systems where the library automatically loads configuration files from the C:\etc directory, which can be created and modified by unprivileged local users.	2026-04-07	7.8
CVE-2026-28261	dell - multiple products	Dell Elastic Cloud Storage, version 3.8.1.7 and prior, and Dell ObjectScale, versions prior to 4.1.0.3 and version 4.2.0.0, contains an Insertion of Sensitive Information into Log File vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to secret exposure. The attacker may be able to use the exposed secret to access the vulnerable system with privileges of the compromised account.	2026-04-08	7.8
CVE-2026-21367	qualcomm - ar8035_firmware	Transient DOS when processing nonstandard FILS Discovery Frames with out-of-range action sizes during initial scans.	2026-04-06	7.6
CVE-2026-21381	qualcomm - ar8035_firmware	Transient DOS when receiving a service data frame with excessive length during device matching over a neighborhood awareness network protocol connection.	2026-04-06	7.6
CVE-2025-57835	samsung - exynos_990_firmware	An issue was discovered in RRC in Samsung Mobile Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 1280, 2200, 1330, 1380, 1480, 2400, 1580, 2500, 9110, W920, W930, W1000, Modem 5123, Modem 5300, and Modem 5400. Improper memory initialization results in an illegal memory access, causing a system crash via a malformed RRCReconfiguration message.	2026-04-06	7.5
CVE-2025-59440	samsung - exynos_990_firmware	An issue was discovered in USIM in Samsung Mobile Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 1280, 2200, 1330, 1380, 1480, 2400, 1580, 2500, 9110, W920, W930, W1000, Modem 5123, Modem 5300, and Modem 5400. Improper handling of SIM card proactive commands leads to a Denial of Service.	2026-04-06	7.5
CVE-2025-54324	samsung - exynos_990_firmware	An issue was discovered in NAS in Samsung Mobile Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 1280, 2200, 1330, 1380, 1480, 2400, 1580, 2500, 9110, W920, W930, W1000, Modem 5123, Modem 5300, and Modem 5400. Incorrect Handling of a DL NAS Transport packet leads to a Denial of Service.	2026-04-06	7.5
CVE-2025-57834	samsung - exynos_980_firmware	An issue was discovered in Samsung Mobile Processor, Wearable Processor, and Modem (Exynos 980, 850, 990, 1080, 2100, 1280, 2200, 1330, 1380, 1480, 2400, 1580, 2500, 1680, 9110, W920, W930, W1000, Modem 5123, Modem 5300, Modem 5400, and Modem 5410). The absence of proper input validation leads to a Denial of Service.	2026-04-06	7.5
CVE-2026-28388	openssl - OpenSSL	Issue summary: When a delta CRL that contains a Delta CRL Indicator extension is processed a NULL pointer dereference might happen if the required CRL Number extension is missing. Impact summary: A NULL pointer dereference can trigger a crash which leads to a Denial of Service for an application. When CRL processing and delta CRL processing is enabled during X.509 certificate verification, the delta CRL processing does not check whether the CRL Number extension is NULL before dereferencing it. When a malformed delta CRL file is being processed, this parameter can be NULL, causing a NULL pointer dereference. Exploiting this issue requires the X509_V_FLAG_USE_DELTAS flag to be enabled in the verification context, the certificate being verified to contain a freshestCRL extension or the base CRL to have the EXFLAG_FRESHEST flag set, and an attacker to provide a malformed CRL to an application that processes it. The vulnerability is limited to Denial of Service and cannot be escalated to achieve code execution or memory disclosure. For that reason the issue was assessed as Low severity according to our Security Policy. The FIPS modules in 3.6, 3.5, 3.4, 3.3 and 3.0 are not affected by this issue, as the affected code is outside the OpenSSL FIPS module boundary.	2026-04-07	7.5
CVE-2026-28389	openssl - OpenSSL	Issue summary: During processing of a crafted CMS EnvelopedData message with KeyAgreeRecipientInfo a NULL pointer dereference can happen.	2026-04-07	7.5

		Impact summary: Applications that process attacker-controlled CMS data may crash before authentication or cryptographic operations occur resulting in Denial of Service. When a CMS EnvelopedData message that uses KeyAgreeRecipientInfo is processed, the optional parameters field of KeyEncryptionAlgorithmIdentifier is examined without checking for its presence. This results in a NULL pointer dereference if the field is missing. Applications and services that call CMS_decrypt() on untrusted input (e.g., S/MIME processing or CMS-based protocols) are vulnerable. The FIPS modules in 3.6, 3.5, 3.4, 3.3 and 3.0 are not affected by this issue, as the affected code is outside the OpenSSL FIPS module boundary.		
CVE-2026-28390	openssl - OpenSSL	Issue summary: During processing of a crafted CMS EnvelopedData message with KeyTransportRecipientInfo a NULL pointer dereference can happen. Impact summary: Applications that process attacker-controlled CMS data may crash before authentication or cryptographic operations occur resulting in Denial of Service. When a CMS EnvelopedData message that uses KeyTransportRecipientInfo with RSA-OAEP encryption is processed, the optional parameters field of RSA-OAEP SourceFunc algorithm identifier is examined without checking for its presence. This results in a NULL pointer dereference if the field is missing. Applications and services that call CMS_decrypt() on untrusted input (e.g., S/MIME processing or CMS-based protocols) are vulnerable. The FIPS modules in 3.6, 3.5, 3.4, 3.3 and 3.0 are not affected by this issue, as the affected code is outside the OpenSSL FIPS module boundary.	2026-04-07	7.5
CVE-2026-31790	openssl - OpenSSL	Issue summary: Applications using RSASVE key encapsulation to establish a secret encryption key can send contents of an uninitialized memory buffer to a malicious peer. Impact summary: The uninitialized buffer might contain sensitive data from the previous execution of the application process which leads to sensitive data leakage to an attacker. RSA_public_encrypt() returns the number of bytes written on success and -1 on error. The affected code tests only whether the return value is non-zero. As a result, if RSA encryption fails, encapsulation can still return success to the caller, set the output lengths, and leave the caller to use the contents of the ciphertext buffer as if a valid KEM ciphertext had been produced. If applications use EVP_PKEY_encapsulate() with RSA/RSASVE on an attacker-supplied invalid RSA public key without first validating that key, then this may cause stale or uninitialized contents of the caller-provided ciphertext buffer to be disclosed to the attacker in place of the KEM ciphertext. As a workaround calling EVP_PKEY_public_check() or EVP_PKEY_public_check_quick() before EVP_PKEY_encapsulate() will mitigate the issue. The FIPS modules in 3.6, 3.5, 3.4, 3.3, 3.1 and 3.0 are affected by this issue.	2026-04-07	7.5
CVE-2025-62188	apache - dolphinscheduler	An Exposure of Sensitive Information to an Unauthorized Actor vulnerability exists in Apache DolphinScheduler. This vulnerability may allow unauthorized actors to access sensitive information, including database credentials. This issue affects Apache DolphinScheduler versions 3.1.*. Users are recommended to upgrade to:	2026-04-09	7.5

		* version ≥ 3.2.0 if using 3.1.x
		
		As a temporary workaround, users who cannot upgrade immediately may restrict the exposed management endpoints by setting the following environment variable:
		
		``
		MANAGEMENT_ENDPOINTS_WEB_EXPOSURE_INCLUDE=health,metrics,prometheus
		``
		
		Alternatively, add the following configuration to the application.yaml file:
		
		``
		management:
		  endpoints:
		  web:
		  exposure:
		  include: health,metrics,prometheus
		``
		
		This issue has been reported as CVE-2023-48796:
		
		https://cveprocess.apache.org/cve5/CVE-2023-48796		

CVE-2026-33266	apache - openmeetings	Use of Hard-coded Cryptographic Key vulnerability in Apache OpenMeetings. The remember-me cookie encryption key is set to default value in openmeetings.properties and not being auto-rotated. In case OM admin hasn't changed the default encryption key, an attacker who has stolen a cookie from a logged-in user can get full user credentials. This issue affects Apache OpenMeetings: from 6.1.0 before 9.0.0. Users are recommended to upgrade to version 9.0.0, which fixes the issue.	2026-04-09	7.5
CVE-2026-34020	apache - openmeetings	Use of GET Request Method With Sensitive Query Strings vulnerability in Apache OpenMeetings. The REST login endpoint uses HTTP GET method with username and password passed as query parameters. Please check references regarding possible impact This issue affects Apache OpenMeetings: from 3.1.3 before 9.0.0. Users are recommended to upgrade to version 9.0.0, which fixes the issue.	2026-04-09	7.5
CVE-2026-40046	apache software foundation - multiple products	Integer Overflow or Wraparound vulnerability in Apache ActiveMQ, Apache ActiveMQ All, Apache ActiveMQ MQTT. The fix for "CVE-2025-66168: MQTT control packet remaining length field is not properly validated" was only applied to 5.19.2 (and future 5.19.x) releases but was missed for all 6.0.0+ versions. This issue affects Apache ActiveMQ: from 6.0.0 before 6.2.4; Apache ActiveMQ All: from 6.0.0 before 6.2.4; Apache ActiveMQ MQTT: from 6.0.0 before 6.2.4. Users are recommended to upgrade to version 6.2.4 or a 5.19.x version starting with 5.19.2 or later (currently latest is 5.19.5), which fixes the issue.	2026-04-09	7.5
CVE-2026-1584	red hat - multiple products	A flaw was found in gnutls. A remote, unauthenticated attacker can exploit this vulnerability by sending a specially crafted ClientHello message with an invalid Pre-Shared Key (PSK) binder value during the TLS handshake. This can lead to a NULL pointer dereference, causing the server to crash and resulting in a remote Denial of Service (DoS) condition.	2026-04-09	7.5
CVE-2026-24880	apache - multiple products	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling') vulnerability in Apache Tomcat via invalid chunk extension.	2026-04-09	7.5

		This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.18, from 10.1.0-M1 through 10.1.52, from 9.0.0.M1 through 9.0.115, from 8.5.0 through 8.5.100, from 7.0.0 through 7.0.109. Other, unsupported versions may also be affected. Users are recommended to upgrade to version 11.0.20, 10.1.52 or 9.0.116, which fix the issue.		
CVE-2026-29129	apache - multiple products	Configured cipher preference order not preserved vulnerability in Apache Tomcat. This issue affects Apache Tomcat: from 11.0.16 through 11.0.18, from 10.1.51 through 10.1.52, from 9.0.114 through 9.0.115. Users are recommended to upgrade to version 11.0.20, 10.1.53 or 9.0.116, which fix the issue.	2026-04-09	7.5
CVE-2026-29146	apache - multiple products	Padding Oracle vulnerability in Apache Tomcat's EncryptInterceptor with default configuration. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.18, from 10.0.0-M1 through 10.1.52, from 9.0.13 through 9..115, from 8.5.38 through 8.5.100, from 7.0.100 through 7.0.109. Users are recommended to upgrade to version 11.0.19, 10.1.53 and 9.0.116, which fixes the issue.	2026-04-09	7.5
CVE-2026-34483	apache - multiple products	Improper Encoding or Escaping of Output vulnerability in the JsonAccessLogValve component of Apache Tomcat. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.20, from 10.1.0-M1 through 10.1.53, from 9.0.40 through 9.0.116. Users are recommended to upgrade to version 11.0.21, 10.1.54 or 9.0.117 , which fix the issue.	2026-04-09	7.5
CVE-2026-34486	apache - multiple products	Missing Encryption of Sensitive Data vulnerability in Apache Tomcat due to the fix for CVE-2026-29146 allowing the bypass of the EncryptInterceptor. This issue affects Apache Tomcat: 11.0.20, 10.1.53, 9.0.116. Users are recommended to upgrade to version 11.0.21, 10.1.54 or 9.0.117, which fix the issue.	2026-04-09	7.5
CVE-2026-34487	apache - multiple products	Insertion of Sensitive Information into Log File vulnerability in the cloud membership for clustering component of Apache Tomcat exposed the Kubernetes bearer token. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.20, from 10.1.0-M1 through 10.1.53, from 9.0.13 through 9.0.116. Users are recommended to upgrade to version 11.0.21, 10.1.54 or 9.0.117, which fix the issue.	2026-04-09	7.5
CVE-2026-22750	vmware - Spring Cloud Gateway	When configuring SSL bundles in Spring Cloud Gateway by using the configuration property spring.ssl.bundle, the configuration was silently ignored and the default SSL configuration was used instead. Note: The 4.2.x branch is no longer under open source support. If you are using Spring Cloud Gateway 4.2.0 and are not an enterprise customer, you can upgrade to any Spring Cloud Gateway 4.2.x release newer than 4.2.0 available on Maven Centeral https://repo1.maven.org/maven2/org/springframework/cloud/spring-cloud-gateway/ . Ideally if you are not an enterprise customer, you should be upgrading to 5.0.2 or 5.1.1 which are the current supported open source releases.	2026-04-10	7.5
CVE-2026-39304	apache software foundation - multiple products	Denial of Service via Out of Memory vulnerability in Apache ActiveMQ Client, Apache ActiveMQ Broker, Apache ActiveMQ. ActiveMQ NIO SSL transports do not correctly handle TLSv1.3 handshake KeyUpdates triggered by clients. This makes it possible for a client to rapidly trigger updates which causes the broker to exhaust all its memory in the SSL engine leading to DoS. Note: TLS versions before TLSv1.3 (such as TLSv1.2) are broken but are not vulnerable to OOM. Previous TLS versions require a full handshake renegotiation which causes a connection to hang but not OOM. This is fixed as well. This issue affects Apache ActiveMQ Client: before 5.19.4, from 6.0.0 before 6.2.4; Apache ActiveMQ Broker: before 5.19.4, from 6.0.0 before 6.2.4; Apache ActiveMQ: before 5.19.4, from 6.0.0 before 6.2.4. Users are recommended to upgrade to version 6.2.4 or 5.19.5, which fixes the issue.	2026-04-10	7.5
CVE-2026-5815	d-link - DIR-645	A vulnerability was detected in D-Link DIR-645 1.01/1.02/1.03. Impacted is the function hedwigcgi_main of the file /cgi-bin/hedwig.cgi. The manipulation results in stack-based buffer overflow. The attack can be launched remotely. The exploit is now	2026-04-09	7.4

		public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.		
CVE-2026-5979	d-link - DIR-605L	A vulnerability was detected in D-Link DIR-605L 2.13B01. Affected by this vulnerability is the function formVirtualServ of the file /goform/formVirtualServ of the component POST Request Handler. The manipulation of the argument curTime results in buffer overflow. The attack can be launched remotely. The exploit is now public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	2026-04-09	7.4
CVE-2026-5980	d-link - DIR-605L	A flaw has been found in D-Link DIR-605L 2.13B01. Affected by this issue is the function formSetMACFilter of the file /goform/formSetMACFilter of the component POST Request Handler. This manipulation of the argument curTime causes buffer overflow. The attack may be initiated remotely. The exploit has been published and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	2026-04-09	7.4
CVE-2026-5981	d-link - DIR-605L	A vulnerability has been found in D-Link DIR-605L 2.13B01. This affects the function formAdvFirewall of the file /goform/formAdvFirewall of the component POST Request Handler. Such manipulation of the argument curTime leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	2026-04-09	7.4
CVE-2026-5982	d-link - DIR-605L	A vulnerability was found in D-Link DIR-605L 2.13B01. This vulnerability affects the function formAdvNetwork of the file /goform/formAdvNetwork of the component POST Request Handler. Performing a manipulation of the argument curTime results in buffer overflow. Remote exploitation of the attack is possible. The exploit has been made public and could be used. This vulnerability only affects products that are no longer supported by the maintainer.	2026-04-09	7.4
CVE-2026-5983	d-link - DIR-605L	A vulnerability was determined in D-Link DIR-605L 2.13B01. This issue affects the function formSetDDNS of the file /goform/formSetDDNS of the component POST Request Handler. Executing a manipulation of the argument curTime can lead to buffer overflow. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized. This vulnerability only affects products that are no longer supported by the maintainer.	2026-04-09	7.4
CVE-2026-5984	d-link - DIR-605L	A vulnerability was identified in D-Link DIR-605L 2.13B01. Impacted is the function formSetLog of the file /goform/formSetLog of the component POST Request Handler. The manipulation of the argument curTime leads to buffer overflow. The attack is possible to be carried out remotely. The exploit is publicly available and might be used. This vulnerability only affects products that are no longer supported by the maintainer.	2026-04-09	7.4
CVE-2026-6012	d-link - DIR-513	A security vulnerability has been detected in D-Link DIR-513 1.10. This affects the function formSetPassword of the file /goform/formSetPassword of the component POST Request Handler. The manipulation of the argument curTime leads to buffer overflow. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	2026-04-10	7.4
CVE-2026-6013	d-link - DIR-513	A vulnerability was detected in D-Link DIR-513 1.10. This vulnerability affects the function formSetRoute of the file /goform/formSetRoute of the component POST Request Handler. The manipulation of the argument curTime results in buffer overflow. The attack may be performed from remote. The exploit is now public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	2026-04-10	7.4
CVE-2026-6014	d-link - DIR-513	A flaw has been found in D-Link DIR-513 1.10. This issue affects the function formAdvanceSetup of the file /goform/formAdvanceSetup of the component POST Request Handler. This manipulation of the argument webpage causes buffer overflow. It is possible to initiate the attack remotely. The exploit has been published and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	2026-04-10	7.4
CVE-2026-30814	tp-link - archer_ax53_firmware	A stack-based buffer overflow in the tmpServer module of TP-Link Archer AX53 v1.0 allows an authenticated adjacent attacker to trigger a segmentation fault and potentially execute arbitrary code via a specially crafted configuration file. Successful exploitation may cause a crash and could allow arbitrary code execution, enabling modification of device state, exposure of sensitive data, or further compromise of device integrity. This issue affects AX53 v1.0: before 1.7.1 Build 20260213.	2026-04-08	7.3
CVE-2026-5844	d-link - DIR-882	A vulnerability was found in D-Link DIR-882 1.01B02. Impacted is the function sprintf of the file prog.cgi of the component HNAP1 SetNetworkSettings Handler. The manipulation of the argument IPAddress results in os command injection. The attack may be performed from remote. The exploit has been made public and could be used. This vulnerability only affects products that are no longer supported by the maintainer.	2026-04-09	7.3
CVE-2026-1343	ibm - multiple products	IBM Verify Identity Access Container 11.0 through 11.0.2 and IBM Security Verify Access Container 10.0 through 10.0.9.1 and IBM Verify Identity Access 11.0 through 11.0.2 and IBM Security Verify Access 10.0 through 10.0.9.1 allows an attacker to contact internal authentication endpoints which are protected by the Reverse Proxy.	2026-04-08	7.2

CVE-2026-4113	sonicwall - SMA1000	An observable response discrepancy vulnerability in the SonicWall SMA1000 series appliances allows a remote attacker to enumerate SSL VPN user credentials.	2026-04-09	7.2
CVE-2026-4116	sonicwall - SMA1000	Improper handling of Unicode encoding in SonicWall SMA1000 series appliances allows a remote authenticated SSLVPN user to bypass Workplace/Connect Tunnel TOTP authentication.	2026-04-09	7.2
CVE-2025-47400	qualcomm - pandeiro_firmware	Cryptographic issue while copying data to a destination buffer without validating its size.	2026-04-06	7.1
CVE-2026-32589	red hat - multiple products	A flaw was found in Red Hat Quay's container image upload process. An authenticated user with push access to any repository on the registry can interfere with image uploads in progress by other users, including those in repositories they do not have access to. This could allow the attacker to read, modify, or cancel another user's in-progress image upload.	2026-04-08	7.1
CVE-2026-32590	red hat - multiple products	A flaw was found in Red Hat Quay's handling of resumable container image layer uploads. The upload process stores intermediate data in the database using a format that, if tampered with, could allow an attacker to execute arbitrary code on the Quay server.	2026-04-08	7.1
CVE-2026-21919	juniper - multiple products	An Incorrect Synchronization vulnerability in the management daemon (mgd) of Juniper Networks Junos OS and Junos OS Evolved allows a network-based attacker with low privileges to cause a complete Denial-of-Service (DoS) of the management plane. When NETCONF sessions are quickly established and disconnected, a locking issue causes mgd processes to hang in an unusable state. When the maximum number of mgd processes has been reached, no new logins are possible. This leads to the inability to manage the device and requires a power-cycle to recover. This issue can be monitored by checking for mgd processes in lockf state in the output of 'show system processes extensive': user@host> show system processes extensive | match mgd <pid> root 20 0 501M 4640K lockf 1 0:01 0.00% mgd If the system still can be accessed (either via the CLI or as root, which might still be possible as last resort as this won't invoke mgd), mgd processes in this state can be killed with 'request system process terminate <PID>' from the CLI or with 'kill -9 <PID>' from the shell. This issue affects: Junos OS: * 23.4 versions before 23.4R2-S4, * 24.2 versions before 24.2R2-S1, * 24.4 versions before 24.4R1-S3, 24.4R2; This issue does not affect Junos OS versions before 23.4R1; Junos OS Evolved: * 23.4 versions before 23.4R2-S5-EVO, * 24.2 versions before 24.2R2-S1-EVO, * 24.4 versions before 24.4R1-S3-EVO, 24.4R2-EVO. This issue does not affect Junos OS Evolved versions before 23.4R1-EVO;	2026-04-09	7.1
CVE-2026-33775	juniper - multiple products	A Missing Release of Memory after Effective Lifetime vulnerability in the BroadBand Edge subscriber management daemon (bbe-smgd) of Juniper Networks Junos OS on MX Series allows an adjacent, unauthenticated attacker to cause a Denial of Service (DoS).	2026-04-09	7.1

		If the authentication packet-type option is configured and a received packet does not match that packet type, the memory leak occurs. When all memory available to bbe-smgd has been consumed, no new subscribers will be able to login. The memory utilization of bbe-smgd can be monitored with the following show command: user@host> show system processes extensive | match bbe-smgd The below log message can be observed when this limit has been reached: bbesmgd[<PID>]: %DAEMON-3-SMD_DPROF_RSMON_ERROR: Resource unavailability, Reason: Daemon Heap Memory exhaustion This issue affects Junos OS on MX Series: * all versions before 22.4R3-S8, * 23.2 versions before 23.2R2-S5, * 23.4 versions before 23.4R2-S6, * 24.2 versions before 24.2R2-S2, * 24.4 versions before 24.4R2, * 25.2 versions before 25.2R2.		
CVE-2026-33780	juniper - multiple products	A Missing Release of Memory after Effective Lifetime vulnerability in the Layer 2 Address Learning Daemon (l2ald) of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent, unauthenticated attacker to cause a memory leak ultimately leading to a Denial of Service (DoS). In an EVPN-MPLS scenario, routes learned from remote multi-homed Provider Edge (PE) devices are programmed as ESI routes. Due to a logic issue in the l2ald memory management, memory allocated for these routes is not released when there is churn for these routes. As a result, memory leaks in the l2ald process which will ultimately lead to a crash and restart of l2ald. Use the following command to monitor the memory consumption by l2ald: user@device> show system process extensive | match "PID|l2ald" This issue affects: Junos OS: * all versions before 22.4R3-S5, * 23.2 versions before 23.2R2-S3, * 23.4 versions before 23.4R2-S4, * 24.2 versions before 24.2R2; Junos OS Evolved: * all versions before 22.4R3-S5-EVO, * 23.2 versions before 23.2R2-S3-EVO, * 23.4 versions before 23.4R2-S4-EVO, * 24.2 versions before 24.2R2-EVO.	2026-04-09	7.1
CVE-2026-33781	juniper - multiple products	An Improper Check for Unusual or Exceptional Conditions vulnerability in the packet forwarding engine (pfe) of Juniper Networks Junos OS on specific EX and QFX Series devices allow an unauthenticated, adjacent attacker to cause a complete Denial of Service (DoS). On EX4k, and QFX5k platforms configured as service-provider edge devices, if L2PT is enabled on the UNI and VSTP is enabled on NNI in VXLAN scenarios, receiving VSTP BPDUs on UNI leads to packet buffer allocation failures, resulting in the device to not pass traffic anymore until it is manually recovered with a restart.This issue affects Junos OS:	2026-04-09	7.1

		* 24.4 releases before 24.4R2, * 25.2 releases before 25.2R1-S1, 25.2R2. This issue does not affect Junos OS releases before 24.4R1.		
CVE-2026-33783	juniper - multiple products	A Function Call With Incorrect Argument Type vulnerability in the sensor interface of Juniper Networks Junos OS Evolved on PTX Series allows a network-based, authenticated attacker with low privileges to cause a complete Denial of Service (DoS). If colored SRTE policy tunnels are provisioned via PCEP, and gRPC is used to monitor traffic in these tunnels, evo-aftmand crashes and doesn't restart which leads to a complete and persistent service impact. The system has to be manually restarted to recover. The issue is seen only when the Originator ASN field in PCEP contains a value larger than 65,535 (32-bit ASN). The issue is not reproducible when SRTE policy tunnels are statically configured. This issue affects Junos OS Evolved on PTX Series: * all versions before 22.4R3-S9-EVO, * 23.2 versions before 23.2R2-S6-EVO, * 23.4 versions before 23.4R2-S7-EVO, * 24.2 versions before 24.2R2-S4-EVO, * 24.4 versions before 24.4R2-S2-EVO, * 25.2 versions before 25.2R1-S2-EVO, 25.2R2-EVO.	2026-04-09	7.1
CVE-2026-33797	juniper - multiple products	An Improper Input Validation vulnerability in Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, adjacent attacker, sending a specific genuine BGP packet in an already established BGP session to reset only that session causing a Denial of Service (DoS). An attacker repeatedly sending the packet will sustain the Denial of Service (DoS).This issue affects Junos OS: * 25.2 versions before 25.2R2 This issue doesn't not affected Junos OS versions before 25.2R1. This issue affects Junos OS Evolved: * 25.2-EVO versions before 25.2R2-EVO This issue doesn't not affected Junos OS Evolved versions before 25.2R1-EVO. eBGP and iBGP are affected. IPv4 and IPv6 are affected.	2026-04-09	7.1
CVE-2025-54602	samsung - exynos_980_firmware	An issue was discovered in the Wi-Fi driver in Samsung Mobile Processor and Wearable Processor Exynos 980, 850, 1080, 1280, 1330, 1380, 1480, 1580, W920, W930, and W1000. Improper synchronization on a global variable leads to a use-after-free. An attacker can trigger a race condition by invoking an ioctl function concurrently from multiple threads.	2026-04-06	7
CVE-2025-54601	samsung - exynos_980_firmware	An issue was discovered in the Wi-Fi driver in Samsung Mobile Processor amd Wearable Processor Exynos 980, 850, 1080, 1280, 1330, 1380, 1480, 1580, W920, W930, and W1000. Improper synchronization on a global variable leads to a double free. An attacker can trigger a race condition by invoking an ioctl function concurrently from multiple threads.	2026-04-06	7
CVE-2026-21916	juniper - multiple products	A UNIX Symbolic Link (Symlink) Following vulnerability in the CLI of Juniper Networks Junos OS allows a local, authenticated attacker with low privileges to escalate their privileges to root which will lead to a complete compromise of the system. When after a user has performed a specific 'file link ...' CLI operation, another user commits (unrelated configuration changes), the first user can login as root. This issue affects Junos OS: * all versions before 23.2R2-S7, * 23.4 versions before 23.4R2-S6,	2026-04-09	7

		* 24.2 versions before 24.2R2-S3, * 24.4 versions before 24.4R2-S2, * 25.2 versions before 25.2R2. This issue does not affect versions 25.4R1 or later.		
CVE-2026-33773	juniper - multiple products	An Incorrect Initialization of Resource vulnerability in the packet forwarding engine (pfe) of Juniper Networks Junos OS on specific EX Series and QFX Series device allows an unauthenticated, network-based attacker to cause an integrity impact to downstream networks. When the same family inet or inet6 filter is applied on an IRB interface and on a physical interface as egress filter on EX4100, EX4400, EX4650 and QFX5120 devices, only one of the two filters will be applied, which can lead to traffic being sent out one of these interfaces which should have been blocked. This issue affects Junos OS on EX Series and QFX Series: * 23.4 version 23.4R2-S6, * 24.2 version 24.2R2-S3. No other Junos OS versions are affected.	2026-04-09	6.9
CVE-2026-34478	apache software foundation - Apache Log4j Core	Apache Log4j Core's Rfc5424Layout https://logging.apache.org/log4j/2.x/manual/layouts.html#RFC5424Layout , in versions 2.21.0 through 2.25.3, is vulnerable to log injection via CRLF sequences due to undocumented renames of security-relevant configuration attributes. Two distinct issues affect users of stream-based syslog services who configure Rfc5424Layout directly: * The newLineEscape attribute was silently renamed, causing newline escaping to stop working for users of TCP framing (RFC 6587), exposing them to CRLF injection in log output. * The useTlsMessageFormat attribute was silently renamed, causing users of TLS framing (RFC 5425) to be silently downgraded to unframed TCP (RFC 6587), without newline escaping. Users of the SyslogAppender are not affected, as its configuration attributes were not modified. Users are advised to upgrade to Apache Log4j Core 2.25.4, which corrects this issue.	2026-04-10	6.9
CVE-2026-34479	apache software foundation - Apache Log4j 1 to Log4j 2 bridge	The Log4j1XmlLayout from the Apache Log4j 1-to-Log4j 2 bridge fails to escape characters forbidden by the XML 1.0 standard, producing malformed XML output. Conforming XML parsers are required to reject documents containing such characters with a fatal error, which may cause downstream log processing systems to drop or fail to index affected records. Two groups of users are affected: * Those using Log4j1XmlLayout directly in a Log4j Core 2 configuration file. * Those using the Log4j 1 configuration compatibility layer with org.apache.log4j.xml.XMLLayout specified as the layout class. Users are advised to upgrade to Apache Log4j 1-to-Log4j 2 bridge version 2.25.4, which corrects this issue. Note: The Apache Log4j 1-to-Log4j 2 bridge is deprecated and will not be present in Log4j 3. Users are encouraged to consult the Log4j 1 to Log4j 2 migration guide https://logging.apache.org/log4j/2.x/migrate-from-log4j1.html , and specifically the section on eliminating reliance on the bridge.	2026-04-10	6.9
CVE-2026-34480	apache software foundation - Apache Log4j Core	Apache Log4j Core's XmlLayout https://logging.apache.org/log4j/2.x/manual/layouts.html#XmlLayout , in versions up to and including 2.25.3, fails to sanitize characters forbidden by the XML 1.0 specification https://www.w3.org/TR/xml/#charsets producing invalid XML output whenever a log message or MDC value contains such characters. The impact depends on the StAX implementation in use: * JRE built-in StAX: Forbidden characters are silently written to the output, producing malformed XML. Conforming parsers must reject such documents with a fatal error, which may cause downstream log-processing systems to drop the affected records. * Alternative StAX implementations (e.g., Woodstox	2026-04-10	6.9

		https://github.com/FasterXML/woodstox , a transitive dependency of the Jackson XML Dataformat module): An exception is thrown during the logging call, and the log event is never delivered to its intended appender, only to Log4j's internal status logger. Users are advised to upgrade to Apache Log4j Core 2.25.4, which corrects this issue by sanitizing forbidden characters before XML output.		
CVE-2026-30816	tp-link - archer_ax53_firmware	An external control of configuration vulnerability in the OpenVPN module of TP-Link AX53 v1.0 allows an authenticated adjacent attacker to read arbitrary file when a malicious configuration file is processed. Successful exploitation may allow unauthorized access to arbitrary files on the device, potentially exposing sensitive information.This issue affects AX53 v1.0: before 1.7.1 Build 20260213.	2026-04-08	6.8
CVE-2026-30817	tp-link - archer_ax53_firmware	An external configuration control vulnerability in the OpenVPN module of TP-Link AX53 v1.0 allows an authenticated adjacent attacker to read arbitrary files when a malicious configuration file is processed. Successful exploitation may allow unauthorized access to arbitrary files on the device, potentially exposing sensitive information.This issue affects AX53 v1.0: before 1.7.1 Build 20260213.	2026-04-08	6.8
CVE-2026-5893	google - chrome	Race in V8 in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	2026-04-08	6.8
CVE-2026-33776	juniper - multiple products	A Missing Authorization vulnerability in the CLI of Juniper Networks Junos OS and Junos OS Evolved allows a local user with low privileges to read sensitive information. A local user with low privileges can execute the CLI command 'show mgd' with specific arguments which will expose sensitive information. This issue affects Junos OS: * all versions before 22.4R3-S8, * 23.2 versions before 23.2R2-S6, * 23.4 versions before 23.4R2-S6, * 24.2 versions before 24.2R2-S4, * 24.4 versions before 24.4R2-S1, * 25.2 version before 25.2R1-S2, 25.2R2; Junos OS Evolved: * all versions before 23.2R2-S6-EVO, * 23.4 version before 23.4R2-S6-EVO, * 24.2 version before 24.2R2-S4-EVO, * 24.4 versions before 24.4R2-S1-EVO, * 25.2 versions before 25.2R2-EVO.	2026-04-09	6.8
CVE-2026-33786	juniper - multiple products	An Improper Check for Unusual or Exceptional Conditions vulnerability in the chassis control daemon (chassisd) of Juniper Networks Junos OS on SRX1600, SRX2300 and SRX4300 allows a local attacker with low privileges to cause a complete Denial of Service (DoS). When a specific 'show chassis' CLI command is executed, chassisd crashes and restarts which causes a momentary impact to all traffic until all modules are online again. This issue affects Junos OS on SRX1600, SRX2300 and SRX4300: * 24.4 versions before 24.4R1-S3, 24.4R2. This issue does not affect Junos OS versions before 24.4R1.	2026-04-09	6.8
CVE-2026-33787	juniper - multiple products	An Improper Check for Unusual or Exceptional Conditions vulnerability in the chassis control daemon (chassisd) of Juniper Networks Junos OS on SRX1500, SRX4100, SRX4200 and SRX4600 allows a local attacker with low privileges to cause a complete Denial of Service (DoS). When a specific 'show chassis' CLI command is executed, chassisd crashes and restarts which causes a momentary impact to all traffic until all modules are online again.	2026-04-09	6.8

		This issue affects Junos OS on SRX1500, SRX4100, SRX4200 and SRX4600: * 23.2 versions before 23.2R2-S6, * 23.4 versions before 23.4R2-S7 * 24.2 versions before 24.2R2-S2, * 24.4 versions before 24.4R2, * 25.2 versions before 25.2R1-S1, 25.2R2.		
CVE-2026-4878	red hat - multiple products	A flaw was found in libcap. A local unprivileged user can exploit a Time-of-check-to-time-of-use (TOCTOU) race condition in the `cap_set_file()` function. This allows an attacker with write access to a parent directory to redirect file capability updates to an attacker-controlled file. By doing so, capabilities can be injected into or stripped from unintended executables, leading to privilege escalation.	2026-04-09	6.7
CVE-2026-27102	dell - multiple products	Dell PowerScale OneFS, versions 9.5.0.0 through 9.10.1.6 and versions 9.11.0.0 through 9.13.0.1, contains an incorrect privilege assignment vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to elevation of privileges.	2026-04-08	6.6
CVE-2026-5892	google - chrome	Insufficient policy enforcement in PWAs in Google Chrome prior to 147.0.7727.55 allowed a remote attacker who had compromised the renderer process to install a PWA without user consent via a crafted HTML page. (Chromium security severity: Medium)	2026-04-08	6.6
CVE-2025-47374	qualcomm - fastconnect_6900_firmware	Memory Corruption when accessing freed memory due to concurrent fence deregistration and signal handling.	2026-04-06	6.5
CVE-2026-32588	apache - multiple products	Authenticated DoS over CQL in Apache Cassandra 4.0, 4.1, 5.0 allows authenticated user to raise query latencies via repeated password changes. Users are recommended to upgrade to version 4.0.20, 4.1.11, 5.0.7, which fixes this issue.	2026-04-07	6.5
CVE-2026-2377	red hat - multiple products	A flaw was found in mirror-registry. Authenticated users can exploit the log export feature by providing a specially crafted web address (URL). This allows the application's backend to make arbitrary requests to internal network resources, a vulnerability known as Server-Side Request Forgery (SSRF). This could lead to unauthorized access to sensitive information or other internal systems.	2026-04-08	6.5
CVE-2026-5876	google - chrome	Side-channel information leakage in Navigation in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-04-08	6.5
CVE-2026-5881	google - chrome	Policy bypass in LocalNetworkAccess in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium)	2026-04-08	6.5
CVE-2026-5885	google - chrome	Insufficient validation of untrusted input in WebML in Google Chrome on Windows prior to 147.0.7727.55 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	2026-04-08	6.5
CVE-2026-5888	google - chrome	Uninitialized Use in WebCodecs in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	2026-04-08	6.5
CVE-2026-5901	google - chrome	Insufficient policy enforcement in DevTools in Google Chrome prior to 147.0.7727.55 allowed an attacker who convinced a user to install a malicious extension to bypass enterprise host restrictions for cookie modification via a crafted Chrome Extension. (Chromium security severity: Low)	2026-04-08	6.5
CVE-2026-5903	google - chrome	Policy bypass in IFrameSandbox in Google Chrome prior to 147.0.7727.55 allowed a remote attacker who convinced a user to engage in specific UI gestures to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	2026-04-08	6.5
CVE-2026-5905	google - chrome	Incorrect security UI in Permissions in Google Chrome on Windows prior to 147.0.7727.55 allowed a remote attacker to perform domain spoofing via a crafted HTML page. (Chromium security severity: Low)	2026-04-08	6.5
CVE-2026-5919	google - chrome	Insufficient validation of untrusted input in WebSockets in Google Chrome prior to 147.0.7727.55 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page. (Chromium security severity: Low)	2026-04-08	6.5
CVE-2026-34538	apache - airflow	Apache Airflow versions 3.0.0 through 3.1.8 DagRun wait endpoint returns XCom result values even to users who only have DAG Run read permissions, such as the Viewer role.This behavior conflicts with the FAB RBAC model, which treats XCom as a separate protected resource, and with the security model documentation that defines the Viewer role as read-only. Airflow uses the FAB Auth Manager to manage access control on a per-resource basis. The Viewer role is intended to be read-only by default, and the security model documentation defines Viewer users as those who can inspect DAGs without accessing sensitive execution results. Users are recommended to upgrade to Apache Airflow 3.2.0 which resolves this issue.	2026-04-09	6.5

CVE-2026-34500	apache - multiple products	CLIENT_CERT authentication does not fail as expected for some scenarios when soft fail is disabled and FFM is used in Apache Tomcat. This issue affects Apache Tomcat: from 11.0.0-M14 through 11.0.20, from 10.1.22 through 10.1.53, from 9.0.92 through 9.0.116. Users are recommended to upgrade to version 11.0.21, 10.1.54 or 9.0.117, which fixes the issue.	2026-04-09	6.5
CVE-2021-47960	synology - Synology SSL VPN Client	A files or directories accessible to external parties vulnerability in Synology SSL VPN Client before 1.4.5-0684 allows remote attackers to access files within the installation directory via a local HTTP server bound to the loopback interface. By leveraging user interaction with a crafted web page, attackers may retrieve sensitive files such as configuration files, certificates, and logs, leading to information disclosure.	2026-04-10	6.5
CVE-2026-33727	pi-hole - pi-hole	Pi-hole is a Linux network-level advertisement and Internet tracker blocking application. Version 6.4 has a local privilege-escalation vulnerability allows code execution as root from the low-privilege pihole account. Important context: the pihole account uses nologin, so this is not a direct interactive-login issue. However, nologin does not prevent code from running as UID pihole if a Pi-hole component is compromised. In that realistic post-compromise scenario, attacker-controlled content in /etc/pihole/versions is sourced by root-run Pi-hole scripts, leading to root code execution. This vulnerability is fixed in 6.4.1.	2026-04-06	6.4
CVE-2025-57847	red hat - multiple products	A container privilege escalation flaw was found in certain Ansible Automation Platform images. This issue arises from the /etc/passwd file being created with group-writable permissions during the build process. In certain conditions, an attacker who can execute commands within an affected container, even as a non-root user, can leverage their membership in the root group to modify the /etc/passwd file. This vulnerability allows an attacker to add a new user with any arbitrary UID, including UID 0, gaining full root privileges within the container.	2026-04-08	6.4
CVE-2025-57851	red hat - multiple products	A container privilege escalation flaw was found in certain Multicluster Engine for Kubernetes images. This issue stems from the /etc/passwd file being created with group-writable permissions during build time. In certain conditions, an attacker who can execute commands within an affected container, even as a non-root user, can leverage their membership in the root group to modify the /etc/passwd file. This could allow the attacker to add a new user with any arbitrary UID, including UID 0, leading to full root privileges within the container.	2026-04-08	6.4
CVE-2025-57853	red hat - Red Hat Web Terminal	A container privilege escalation flaw was found in certain Web Terminal images. This issue stems from the /etc/passwd file being created with group-writable permissions during build time. In certain conditions, an attacker who can execute commands within an affected container, even as a non-root user, can leverage their membership in the root group to modify the /etc/passwd file. This could allow the attacker to add a new user with any arbitrary UID, including UID 0, leading to full root privileges within the container.	2026-04-08	6.4
CVE-2025-57854	red hat - Red Hat OpenShift Update Service	A container privilege escalation flaw was found in certain OpenShift Update Service (OSUS) images. This issue stems from the /etc/passwd file being created with group-writable permissions during build time. In certain conditions, an attacker who can execute commands within an affected container, even as a non-root user, may be able to leverage their membership in the root group to modify the /etc/passwd file. This could allow the attacker to add a new user with any arbitrary UID, including UID 0, leading to full root privileges within the container.	2026-04-08	6.4
CVE-2025-58713	red hat - multiple products	A container privilege escalation flaw was found in certain Red Hat Process Automation Manager images. This issue stems from the /etc/passwd file being created with group-writable permissions during build time. In certain conditions, an attacker who can execute commands within an affected container, even as a non-root user, can leverage their membership in the root group to modify the /etc/passwd file. This could allow the attacker to add a new user with any arbitrary UID, including UID 0, leading to full root privileges within the container.	2026-04-08	6.4
CVE-2026-33785	juniper - multiple products	A Missing Authorization vulnerability in the CLI of Juniper Networks Junos OS on MX Series allows a local, authenticated user with low privileges to execute specific commands which will lead to a complete compromise of managed devices. Any user logged in, without requiring specific privileges, can issue 'request csds' CLI operational commands. These commands are only meant to be executed by high privileged or users designated for Juniper Device Manager (JDM) / Connected Security Distributed Services (CSDS) operations as they will impact all aspects of the devices managed via the respective MX. This issue affects Junos OS on MX Series: * 24.4 releases before 24.4R2-S3, * 25.2 releases before 25.2R2. This issue does not affect Junos OS releases before 24.4.	2026-04-09	6.3
CVE-2026-34477	apache software foundation -	The fix for CVE-2025-68161 https://logging.apache.org/security.html#CVE-2025-68161 was incomplete: it addressed hostname verification only when enabled via the log4j2.sslVerifyHostName	2026-04-10	6.3

	Apache Log4j Core	https://logging.apache.org/log4j/2.x/manual/systemproperties.html#log4j2.sslVerifyHostName system property, but not when configured through the verifyHostName https://logging.apache.org/log4j/2.x/manual/appenders/network.html#SslConfiguration-attr-verifyHostName attribute of the <Ssl> element. Although the verifyHostName configuration attribute was introduced in Log4j Core 2.12.0, it was silently ignored in all versions through 2.25.3, leaving TLS connections vulnerable to interception regardless of the configured value. A network-based attacker may be able to perform a man-in-the-middle attack when all of the following conditions are met: * An SMTP, Socket, or Syslog appender is in use. * TLS is configured via a nested <Ssl> element. * The attacker can present a certificate issued by a CA trusted by the appender's configured trust store, or by the default Java trust store if none is configured. This issue does not affect users of the HTTP appender, which uses a separate verifyHostname https://logging.apache.org/log4j/2.x/manual/appenders/network.html#HttpAppender-attr-verifyHostName attribute that was not subject to this bug and verifies host names by default. Users are advised to upgrade to Apache Log4j Core 2.25.4, which corrects this issue.		
CVE-2026-34481	apache software foundation - Apache Log4j JSON Template Layout	Apache Log4j's JsonTemplateLayout https://logging.apache.org/log4j/2.x/manual/json-template-layout.html , in versions up to and including 2.25.3, produces invalid JSON output when log events contain non-finite floating-point values (NaN, Infinity, or -Infinity), which are prohibited by RFC 8259. This may cause downstream log processing systems to reject or fail to index affected records. An attacker can exploit this issue only if both of the following conditions are met: * The application uses JsonTemplateLayout. * The application logs a MapMessage containing an attacker-controlled floating-point value. Users are advised to upgrade to Apache Log4j JSON Template Layout 2.25.4, which corrects this issue.	2026-04-10	6.3
CVE-2026-40021	apache software foundation - Apache Log4net	Apache Log4net's XmlLayout https://logging.apache.org/log4net/manual/configuration/layouts.html#layout-list and XmlLayoutSchemaLog4J https://logging.apache.org/log4net/manual/configuration/layouts.html#layout-list , in versions before 3.3.0, fail to sanitize characters forbidden by the XML 1.0 specification https://www.w3.org/TR/xml/#charsets in MDC property keys and values, as well as the identity field that may carry attacker-influenced data. This causes an exception during serialization and the silent loss of the affected log event. An attacker who can influence any of these fields can exploit this to suppress individual log records, impairing audit trails and detection of malicious activity. Users are advised to upgrade to Apache Log4net 3.3.0, which fixes this issue.	2026-04-10	6.3
CVE-2026-40023	apache software foundation - multiple products	Apache Log4cxx's XMLLayout https://logging.apache.org/log4cxx/1.7.0/classlog4cxx_1_1xml_1_1XMLLayout.html , in versions before 1.7.0, fails to sanitize characters forbidden by the XML 1.0 specification https://www.w3.org/TR/xml/#charsets in log messages, NDC, and MDC property keys and values, producing invalid XML output. Conforming XML parsers must reject such documents with a fatal error, which may cause downstream log processing systems to drop or fail to index affected records. An attacker who can influence logged data can exploit this to suppress individual log records, impairing audit trails and detection of malicious activity. Users are advised to upgrade to Apache Log4cxx 1.7.0, which fixes this issue.	2026-04-10	6.3
CVE-2026-0049	google - multiple products	In onHeaderDecoded of LocalImageResolver.java, 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.	2026-04-06	6.2
CVE-2025-13044	ibm - concert	IBM Concert 1.0.0 through 2.2.0 creates temporary files with predictable names, which allows local users to overwrite arbitrary files via a symlink attack.	2026-04-07	6.2
CVE-2026-33403	pi-hole - web_interface	Pi-hole Admin Interface is a web interface for managing Pi-hole, a network-level ad and internet tracker blocking application. From 6.0 to before 6.5, a reflected DOM-based XSS vulnerability in taillog.js allows an unauthenticated attacker to inject arbitrary HTML into the Pi-hole admin interface by crafting a malicious URL. The file query parameter is interpolated into an innerHTML assignment without escaping. Because the Content-Security-Policy is missing the form-action directive, injected <form> elements can exfiltrate credentials to an external origin. This vulnerability is fixed in 6.5.	2026-04-06	6.1
CVE-2026-35199	microsoft - symcrypt	SymCrypt is the core cryptographic function library currently used by Windows. From 103.5.0 to before 103.11.0, The SymCryptXmssSign function passes a 64-bit leaf count value to a helper function that accepts a 32-bit parameter. For XMSS^MT parameter sets with total tree height >= 32 (which includes standard predefined parameters), this causes silent truncation to zero, resulting in a drastically undersized scratch buffer allocation followed by a heap buffer overflow during signature computation. Exploiting this issue would require an application using SymCrypt to perform an XMSS^MT	2026-04-06	6.1

		signature using an attacker-controlled parameter set. It is uncommon for applications to allow the use of attacker-controlled parameter sets for signing, since signing is a private key operation, and private keys must be trusted by definition. Additionally, XMSS(^MT) signing should only be performed in a Hardware Security Module (HSM). XMSS(^MT) signing is provided in SymCrypt only for testing purposes. This is a general rule irrespective of this CVE; XMSS(^MT) and other stateful signature schemes are only cryptographically secure when it is guaranteed that the same state cannot be reused for two different signatures, which cannot be guaranteed by software alone. For this reason, XMSS(^MT) signing is also not FIPS approved when performed outside of an HSM. Fixed in version 103.11.0.		
CVE-2026-35491	pi-hole - ftldns	FTLDNS (pihole-FTL) provides an interactive API and also generates statistics for Pi-hole's Web interface. From 6.0 to before 6.6, Pi-hole FTL supports a CLI password feature (webserver.api.cli_pw) that creates “CLI” API sessions intended to be read-only for configuration changes. While /api/config correctly blocks CLI sessions from mutating configuration, /api/teleporter allowed Teleporter imports for CLI sessions, enabling a CLI-scoped session to overwrite configuration via a Teleporter archive (authorization bypass). This vulnerability is fixed in 6.6.	2026-04-07	6.1
CVE-2026-5896	google - chrome	Policy bypass in Audio in Google Chrome prior to 147.0.7727.55 allowed a remote attacker who convinced a user to engage in specific UI gestures to bypass sandbox download restrictions via a crafted HTML page. (Chromium security severity: Low)	2026-04-08	6.1
CVE-2026-5899	google - chrome	Insufficient policy enforcement in History Navigation in Google Chrome prior to 147.0.7727.55 allowed a remote attacker who convinced a user to engage in specific UI gestures to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: Low)	2026-04-08	6.1
CVE-2026-25854	apache - multiple products	Occasional URL redirection to untrusted Site ('Open Redirect') vulnerability in Apache Tomcat via the LoadBalancerDrainingValve. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.18, from 10.1.0-M1 through 10.1.52, from 9.0.0.M23 through 9.0.115, from 8.5.30 through 8.5.100. Other, unsupported versions may also be affected Users are recommended to upgrade to version 11.0.20, 10.1.53 or 9.0.116, which fix the issue.	2026-04-09	6.1
CVE-2026-5673	red hat - multiple products	A flaw was found in libtheora. This heap-based out-of-bounds read vulnerability exists within the AVI (Audio Video Interleave) parser, specifically in the avi_parse_input_file() function. A local attacker could exploit this by tricking a user into opening a specially crafted AVI file containing a truncated header sub-chunk. This could lead to a denial-of-service (application crash) or potentially leak sensitive information from the heap.	2026-04-06	5.6
CVE-2025-48651	google - android	In importWrappedKey of KMKeymasterApplet.java, there is a possible way access keys that should be restricted due to improper input validation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-04-06	5.5
CVE-2026-5745	red hat - multiple products	A flaw was found in libarchive. A NULL pointer dereference vulnerability exists in the ACL parsing logic, specifically within the archive_acl_from_text_nl() function. When processing a malformed ACL string (such as a bare "d" or "default" tag without subsequent fields), the function fails to perform adequate validation before advancing the pointer. An attacker can exploit this by providing a maliciously crafted archive, causing an application utilizing the libarchive API (such as bsdtar) to crash, resulting in a Denial of Service (DoS).	2026-04-07	5.5
CVE-2026-27315	apache - cassandra	Sensitive Information Leak in cqlsh in Apache Cassandra 4.0 allows access to sensitive information, like passwords, from previously executed cqlsh command via ~/.cassandra/cqlsh_history local file access. Users are recommended to upgrade to version 4.0.20, which fixes this issue. -- Description: Cassandra's command-line tool, cqlsh, provides a command history feature that allows users to recall previously executed commands using the up/down arrow keys. These history records are saved in the ~/.cassandra/cqlsh_history file in the user's home directory. However, cqlsh does not redact sensitive information when saving command history. This means that if a user executes operations involving passwords (such as logging in or creating users) within cqlsh, these passwords are permanently stored in cleartext in the history file on the disk.	2026-04-07	5.5
CVE-2026-33406	pi-hole - web_interface	Pi-hole Admin Interface is a web interface for managing Pi-hole, a network-level ad and internet tracker blocking application. From 6.0 to before 6.5, configuration values from the /api/config endpoint are placed directly into HTML value="" attributes without escaping in settings-advanced.js, enabling HTML attribute injection. A double quote in any config value breaks out of the attribute context. JavaScript execution is blocked by the server's CSP (script-src 'self'), but injected attributes can alter element styling for UI redressing. The primary attack vector is importing a malicious teleporter backup, which bypasses per-field server-side validation. This vulnerability is fixed in 6.5.	2026-04-06	5.4
CVE-2026-5895	google - chrome	Incorrect security UI in Omnibox in Google Chrome on iOS prior to 147.0.7727.55 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name. (Chromium security severity: Low)	2026-04-08	5.4
CVE-2026-33119	microsoft - edge	User interface (ui) misrepresentation of critical information in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	2026-04-10	5.4

CVE-2025-14243	red hat - multiple products	A flaw was found in the OpenShift Mirror Registry. This vulnerability allows an unauthenticated, remote attacker to enumerate valid usernames and email addresses via different error messages during authentication failures and account creation.	2026-04-08	5.3
CVE-2026-5886	google - chrome	Out of bounds read in WebAudio in Google Chrome on Mac prior to 147.0.7727.55 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	2026-04-08	5.3
CVE-2026-5890	google - chrome	Race in WebCodecs in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	2026-04-08	5.3
CVE-2026-32990	apache - multiple products	Improper Input Validation vulnerability in Apache Tomcat due to an incomplete fix of CVE-2025-66614. This issue affects Apache Tomcat: from 11.0.15 through 11.0.19, from 10.1.50 through 10.1.52, from 9.0.113 through 9.0.115. Users are recommended to upgrade to version 11.0.20, 10.1.53 or 9.0.116, which fix the issue.	2026-04-09	5.3
CVE-2026-32591	red hat - multiple products	A flaw was found in Red Hat Quay's Proxy Cache configuration feature. When an organization administrator configures an upstream registry for proxy caching, Quay makes a network connection to the specified registry hostname without verifying that it points to a legitimate external service. An attacker with organization administrator privileges could supply a crafted hostname to force the Quay server to make requests to internal network services, cloud infrastructure endpoints, or other resources that should not be accessible from the Quay application.	2026-04-08	5.2
CVE-2026-5704	red hat - multiple products	A flaw was found in tar. A remote attacker could exploit this vulnerability by crafting a malicious archive, leading to hidden file injection with fully attacker-controlled content. This bypasses pre-extraction inspection mechanisms, potentially allowing an attacker to introduce malicious files onto a system without detection.	2026-04-06	5
CVE-2026-24511	dell - multiple products	Dell PowerScale OneFS, versions 9.5.0.0 through 9.10.1.6 and versions 9.11.0.0 through 9.13.0.0, contains a generation of error message containing sensitive information vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to information disclosure.	2026-04-08	4.4
CVE-2026-33227	apache software foundation - multiple products	Improper validation and restriction of a classpath path name vulnerability in Apache ActiveMQ Client, Apache ActiveMQ Broker, Apache ActiveMQ All, Apache ActiveMQ Web, Apache ActiveMQ. In two instances (when creating a Stomp consumer and also browsing messages in the Web console) an authenticated user provided "key" value could be constructed to traverse the classpath due to path concatenation. As a result, the application is exposed to a classpath path resource loading vulnerability that could potentially be chained together with another attack to lead to exploit. This issue affects Apache ActiveMQ Client: before 5.19.3, from 6.0.0 before 6.2.2; Apache ActiveMQ Broker: before 5.19.3, from 6.0.0 before 6.2.2; Apache ActiveMQ All: before 5.19.3, from 6.0.0 before 6.2.2; Apache ActiveMQ Web: before 5.19.3, from 6.0.0 before 6.2.2; Apache ActiveMQ: before 5.19.3, from 6.0.0 before 6.2.2. Users are recommended to upgrade to version 5.19.4 or 6.2.3, which fixes the issue. Note: 5.19.3 and 6.2.2 also fix this issue, but that is limited to non-Windows environments due to a path separator resolution bug fixed in 5.19.4 and 6.2.3.	2026-04-07	4.3
CVE-2026-5864	google - chrome	Heap buffer overflow in WebAudio in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	2026-04-08	4.3
CVE-2026-5867	google - chrome	Heap buffer overflow in WebML in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	2026-04-08	4.3
CVE-2026-5869	google - chrome	Heap buffer overflow in WebML in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	2026-04-08	4.3
CVE-2026-5875	google - chrome	Policy bypass in Blink in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	2026-04-08	4.3
CVE-2026-5878	google - chrome	Incorrect security UI in Blink in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	2026-04-08	4.3
CVE-2026-5880	google - chrome	Insufficient policy enforcement in browser UI in Google Chrome prior to 147.0.7727.55 allowed a remote attacker who had compromised the renderer process to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Medium)	2026-04-08	4.3
CVE-2026-5882	google - chrome	Incorrect security UI in Fullscreen in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	2026-04-08	4.3
CVE-2026-5887	google - chrome	Insufficient validation of untrusted input in Downloads in Google Chrome on Windows prior to 147.0.7727.55 allowed a remote attacker to bypass download restrictions via a crafted HTML page. (Chromium security severity: Medium)	2026-04-08	4.3
CVE-2026-5889	google - chrome	Cryptographic Flaw in PDFium in Google Chrome prior to 147.0.7727.55 allowed an attacker to read potentially sensitive information from encrypted PDFs via a brute-force attack. (Chromium security severity: Medium)	2026-04-08	4.3

CVE-2026-5891	google - chrome	Insufficient policy enforcement in browser UI in Google Chrome prior to 147.0.7727.55 allowed a remote attacker who had compromised the renderer process to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	2026-04-08	4.3
CVE-2026-5894	google - chrome	Inappropriate implementation in PDF in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	2026-04-08	4.3
CVE-2026-5897	google - chrome	Incorrect security UI in Downloads in Google Chrome prior to 147.0.7727.55 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	2026-04-08	4.3
CVE-2026-5898	google - chrome	Incorrect security UI in Omnibox in Google Chrome on iOS prior to 147.0.7727.55 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	2026-04-08	4.3
CVE-2026-5900	google - chrome	Policy bypass in Downloads in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to bypass of multi-download protections via a crafted HTML page. (Chromium security severity: Low)	2026-04-08	4.3
CVE-2026-5906	google - chrome	Incorrect security UI in Omnibox in Google Chrome on Android prior to 147.0.7727.55 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Low)	2026-04-08	4.3
CVE-2026-5911	google - chrome	Policy bypass in ServiceWorkers in Google Chrome prior to 147.0.7727.55 allowed a remote attacker to bypass content security policy via a crafted HTML page. (Chromium security severity: Low)	2026-04-08	4.3
CVE-2026-5918	google - chrome	Inappropriate implementation in Navigation in Google Chrome prior to 147.0.7727.55 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	2026-04-08	4.3
CVE-2026-33005	apache - openmeetings	Improper Handling of Insufficient Privileges vulnerability in Apache OpenMeetings. Any registered user can query web service with their credentials and get files/sub-folders of any folder by ID (metadata only NOT contents). Metadata includes id, type, name and some other field. Full list of fields get be checked at FileItemDTO object. This issue affects Apache OpenMeetings: from 3.10 before 9.0.0. Users are recommended to upgrade to version 9.0.0, which fixes the issue.	2026-04-09	4.3
CVE-2026-33118	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Spoofing Vulnerability	2026-04-10	4.3
CVE-2026-37977	red hat - Red Hat Build of Keycloak	A flaw was found in Keycloak. A remote attacker can exploit a Cross-Origin Resource Sharing (CORS) header injection vulnerability in Keycloak's User-Managed Access (UMA) token endpoint. This flaw occurs because the `azp` claim from a client-supplied JSON Web Token (JWT) is used to set the `Access-Control-Allow-Origin` header before the JWT signature is validated. When a specially crafted JWT with an attacker-controlled `azp` value is processed, this value is reflected as the CORS origin, even if the grant is later rejected. This can lead to the exposure of low-sensitivity information from authorization server error responses, weakening origin isolation, but only when a target client is misconfigured with `webOrigins: ["*"]`.	2026-04-06	3.7
CVE-2026-33404	pi-hole - web_interface	Pi-hole Admin Interface is a web interface for managing Pi-hole, a network-level ad and internet tracker blocking application. From 6.0 to before 6.5, client hostnames and IP addresses from the FTL database are rendered into the DOM without escaping in network.js (Network page) and charts.js/index.js (Dashboard chart tooltips). While upstream validation in dnsmasq and FTL blocks HTML characters via normal DHCP/DNS paths, the web UI performs no output escaping — an inconsistency with other fields in the same file that are properly escaped. This vulnerability is fixed in 6.5.	2026-04-06	3.4
CVE-2026-28264	dell - PowerProtect Agent	Dell PowerProtect Agent Service, version(s) prior to 20.1, contain(s) an Incorrect Permission Assignment for Critical Resource vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information exposure.	2026-04-08	3.3
CVE-2026-33405	pi-hole - web_interface	Pi-hole Admin Interface is a web interface for managing Pi-hole, a network-level ad and internet tracker blocking application. From 6.0 to before 6.5, the formatInfo() function in queries.js renders data.upstream, data.client.ip, and data.ede.text into HTML without escaping when a user expands a query row in the Query Log, enabling stored HTML injection. JavaScript execution is blocked by the server's CSP (script-src 'self'). The same fields are properly escaped in the table view (rowCallback), confirming the omission was an oversight. This vulnerability is fixed in 6.5.	2026-04-06	3.1

Where NCA provides the vulnerability information as published by NIST's NVD. In addition, it is the entity's or individual's responsibility to ensure the implementation of appropriate recommendations.

وحيث تقدم الهيئة تفاصيل الثغرات كما تم نشرها من قبل NIST's NVD. وإذ تبقى مسؤولية الجهة أو الشخص قائمة للتأكد من تطبيق التوصيات المناسبة.
