Daily brief, Thursday, April 9, 2026

Apr 8, 8:00 PM to Apr 9, 8:00 PM ET

Generated Nov 7, 2026, 8:13 AM ET

0	0	0	40	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

40 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

No CVEs added to CISA's known-exploited list.

New public exploit code

No new Nuclei templates, Metasploit modules, Exploit-DB or VulnCheck XDB entries.

New critical CVEs

40

9.1 **CVE-2026-29145** Apache Apache Tomcat EXPLOIT CODE

Product not on watchlist.

9.8 **CVE-2026-33784** Juniper virtual lightweight collector

A Use of Default Password vulnerability in the Juniper Networks Support Insights (JSI) Virtual Lightweight Collector (vLWC) allows an unauthenticated, network-based attacker to take full control of the device. vLWC software images ship with an initial password

9.1 **CVE-2026-39980** OpenCTI-Platform opencti

Product not on watchlist.

9.6 **CVE-2026-40088** Praison praisonai

PraisonAI is a multi-agent teams system. Prior to 4.5.121, the execute_command function and workflow shell execution are exposed to user-controlled input via agent workflows, YAML definitions, and LLM-generated tool calls, allowing attackers to inject arbitrar

9.9 **CVE-2025-62718** Axios axios

Axios is a promise based HTTP client for the browser and Node.js. Prior to 1.15.0 and 0.31.0, Axios does not correctly handle hostname normalization when checking NO_PROXY rules. Requests to loopback addresses like localhost. (with a trailing dot) or [::1] (IP

9.9 **CVE-2026-34987** Bytecodealliance wasmtime

Wasmtime is a runtime for WebAssembly. From 25.0.0 to before 36.0.7, 42.0.2, and 43.0.1, Wasmtime with its Winch (baseline) non-default compiler backend may allow properly constructed guest Wasm to access host memory outside of its linear-memory sandbox. This

9.9 **CVE-2026-40089** Sonicverse radio audio streaming stack

Sonicverse is a Self-hosted Docker Compose stack for live radio streaming. The Sonicverse Radio Audio Streaming Stack dashboard contains a Server-Side Request Forgery (SSRF) vulnerability in its API client (apps/dashboard/lib/api.ts). Installations created usi

9.8 **CVE-2026-1830** DETECTION

The Quick Playground plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 1.3.1. This is due to insufficient authorization checks on REST API endpoints that expose a sync code and allow arbitrary file uploads. This

9.8 **CVE-2026-5850** DETECTION

A vulnerability was identified in Totolink A7100RU 7.4cu.2313_b20191024. This affects the function setVpnPassCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. The manipulation of the argument pptpPassThru leads to os command injection. Remote

9.8 **CVE-2026-5851** DETECTION

A security flaw has been discovered in Totolink A7100RU 7.4cu.2313_b20191024. This impacts the function setUPnPCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. The manipulation of the argument enable results in os command injection. The attac

9.8 **CVE-2026-5852** DETECTION

A weakness has been identified in Totolink A7100RU 7.4cu.2313_b20191024. Affected is the function setIptvCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. This manipulation of the argument igmpVer causes os command injection. The attack is pos

9.8 **CVE-2026-5853** DETECTION

A security vulnerability has been detected in Totolink A7100RU 7.4cu.2313_b20191024. Affected by this vulnerability is the function setIpv6LanCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Such manipulation of the argument addrPrefixLen lea

9.8 **CVE-2026-5854** DETECTION

A vulnerability was detected in Totolink A7100RU 7.4cu.2313_b20191024. Affected by this issue is the function setWiFiEasyCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Performing a manipulation of the argument merge results in os command in

9.8 **CVE-2026-5442** Orthanc-Server orthanc

A heap buffer overflow vulnerability exists in the DICOM image decoder. Dimension fields are encoded using Value Representation (VR) Unsigned Long (UL), instead of the expected VR Unsigned Short (US), which allows extremely large dimensions to be processed. Th

9.8 **CVE-2026-5443** Orthanc-Server orthanc

A heap buffer overflow vulnerability exists during the decoding of `PALETTE COLOR` DICOM images. Pixel length validation uses 32-bit multiplication for width and height calculations. If these values overflow, the validation check incorrectly succeeds, allowing

9.8 **CVE-2026-28205** Openplcproject openplc v3 firmware

OpenPLC_V3 is vulnerable to an Initialization of a Resource with an Insecure Default vulnerability which could allow an attacker to gain access to the system by bypassing authentication via an API.

9.8 **CVE-2026-31170** Totolink a3300r firmware

An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the stun-pass parameter to /cgi-bin/cstecgi.cgi.

9.8 **CVE-2025-13926**

An attacker could use data obtained by sniffing the network traffic to forge packets in order to make arbitrary requests to Contemporary Controls BASC 20T.

9.8 **CVE-2026-5187** Wolfssl wolfssl

Two potential heap out-of-bounds write locations existed in DecodeObjectId() in wolfcrypt/src/asn.c. First, a bounds check only validates one available slot before writing two OID arc values (out[0] and out[1]), enabling a 2-byte out-of-bounds write when outSz

9.8 **CVE-2026-5975**

A vulnerability was identified in Totolink A7100RU 7.4cu.2313_b20191024. The impacted element is the function setDmzCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Such manipulation of the argument wanIdx leads to os command injection. The a

20 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches

No new breaches published.

Watch Floor collects CVE records, CISA KEV, exploit indexes, official advisories, security news and chatter. CVSS is the headline score. Ransomware posts are criminal groups' claims, not confirmed by the victims. Leak-site data: RansomLook (ransomlook.io), CC BY 4.0; sectors grouped and countries mapped by Watch Floor. CVE IDs link to the full record on Watch Floor.