Daily brief, Friday, January 2, 2026

Jan 1, 7:00 PM to Jan 2, 7:00 PM ET

Generated Nov 9, 2026, 1:24 AM ET

0	0	0	14	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

14 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

14

9.1 **CVE-2026-21445** Langflow langflow DETECTION

Langflow is a tool for building and deploying AI-powered agents and workflows. Prior to version 1.7.0.dev45, multiple critical API endpoints in Langflow are missing authentication controls. The issue allows any unauthenticated user to access sensitive user con

9.8 **CVE-2025-14998** DETECTION

The Branda plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 3.4.24. This is due to the plugin not properly validating a user's identity prior to updating their password. This makes it possibl

9.8 **CVE-2025-11837** Qnap malware remover

An improper control of generation of code vulnerability has been reported to affect Malware Remover. The remote attackers can then exploit the vulnerability to bypass protection mechanism. We have already fixed the vulnerability in the following version: Malwa

9.8 **CVE-2026-21450** Webkul bagisto

+1 more CVEs in the same release

Bagisto is an open source laravel eCommerce platform. Versions prior to 2.3.10 are vulnerable to server-side template injection via type parameter, which can lead to remote code execution or another exploitation. Version 2.3.10 fixes the issue.

9.2 **CVE-2026-21440**

AdonisJS is a TypeScript-first web framework. A Path Traversal vulnerability in AdonisJS multipart file handling may allow a remote attacker to write arbitrary files to arbitrary locations on the server filesystem. This impacts @adonisjs/bodyparser through ver

9.8 **CVE-2025-67268** Gpsd Project gpsd

gpsd before commit dc966aa contains a heap-based out-of-bounds write vulnerability in the drivers/driver_nmea2000.c file. The hnd_129540 function, which handles NMEA2000 PGN 129540 (GNSS Satellites in View) packets, fails to validate the user-supplied satellit

9.8 **CVE-2025-59389** Qnap hyper data protector

An SQL injection vulnerability has been reported to affect Hyper Data Protector. The remote attackers can then exploit the vulnerability to execute unauthorized code or commands. We have already fixed the vulnerability in the following versions: Hyper Data Pro

9.8 **CVE-2026-21446** Webkul bagisto

Bagisto is an open source laravel eCommerce platform. In versions on the 2.3 branch prior to 2.3.10, API routes remain active even after initial installation is complete. The underlying API endpoints (`/install/api/*`) are directly accessible and exploitable w

9.3 **CVE-2025-64119**

A vulnerability in Nuvation Battery Management System allows Authentication Bypass.This issue affects Battery Management System: through 2.3.9.

9.8 **CVE-2025-64121** Nuvationenergy nplatform

Authentication Bypass Using an Alternate Path or Channel vulnerability in Nuvation Energy Multi-Stack Controller (MSC) allows Authentication Bypass.This issue affects Multi-Stack Controller (MSC): from 2.3.8 before 2.5.1.

9.8 **CVE-2025-65125** Gosaliajainam online-movie-booking

SQL injection in gosaliajainam/online-movie-booking 5.5 in movie_details.php allows attackers to gain sensitive information.

9.8 **CVE-2025-64123** Nuvationenergy nplatform

Unintended Proxy or Intermediary vulnerability in Nuvation Energy Multi-Stack Controller (MSC) allows Network Boundary Bridging.This issue affects Multi-Stack Controller (MSC): through and including release 2.5.1.

9.3 **CVE-2026-21430** Emlog emlog

Emlog is an open source website building system. In version 2.5.23, article creation functionality is vulnerable to cross-site request forgery (CSRF). This can lead to a user being forced to post an article with arbitrary, attacker-controlled content. This, wh

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.