Daily brief, Thursday, February 26, 2026

Feb 25, 7:00 PM to Feb 26, 7:00 PM ET

Generated Nov 7, 2026, 3:44 PM ET

0	0	0	11	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

11 new critical CVEs, 1 new breaches.

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

11

9.9 **CVE-2026-27965** Linuxfoundation vitess

Vitess is a database clustering system for horizontal scaling of MySQL. Prior to versions 23.0.3 and 22.0.4, anyone with read/write access to the backup storage location (e.g. an S3 bucket) can manipulate backup manifest files so that arbitrary code is later e

9.8 **CVE-2026-27966** Langflow langflow

Langflow is a tool for building and deploying AI-powered agents and workflows. Prior to version 1.8.0, the CSV Agent node in Langflow hardcodes `allow_dangerous_code=True`, which automatically exposes LangChain's Python REPL tool (`python_repl_ast`). As a resu

9.8 **CVE-2025-50857**

ZenTaoPMS v18.11 through v21.6.beta is vulnerable to Directory Traversal in /module/ai/control.php. This allows attackers to execute arbitrary code via a crafted file upload

9.1 **CVE-2026-28215** Hoppscotch hoppscotch

hoppscotch is an open source API development ecosystem. Prior to version 2026.2.0, an unauthenticated attacker can overwrite the entire infrastructure configuration of a self-hosted Hoppscotch instance including OAuth provider credentials and SMTP settings by

9.8 **CVE-2026-28213** Evershop evershop

EverShop is a TypeScript-first eCommerce platform. Versions prior to 2.1.1 have a vulnerability in the "Forgot Password" functionality. When specifying a target email address, the API response returns the password reset token. This allows an attacker to take o

9.8 **CVE-2026-22207**

OpenViking through version 0.1.18, prior to commit 0251c70, contains a broken access control vulnerability that allows unauthenticated attackers to gain ROOT privileges when the root_api_key configuration is omitted. Attackers can send requests to protected en

9.1 **CVE-2026-27809** Psd-Tools Project psd-tools

psd-tools is a Python package for working with Adobe Photoshop PSD files. Prior to version 1.12.2, when a PSD file contains malformed RLE-compressed image data (e.g. a literal run that extends past the expected row size), decode_rle() raises ValueError which p

9.9 **CVE-2026-27941** Openlit openlit software development kit

OpenLIT is an open source platform for AI engineering. Prior to version 1.37.1, several GitHub Actions workflows in OpenLIT's GitHub repository use the `pull_request_target` event while checking out and executing untrusted code from forked pull requests. These

9.6 **CVE-2026-27510** Unitree go2 firmware

Unitree Go2 firmware versions 1.1.7 through 1.1.11, when used with the Unitree Go2 Android application (com.unitree.doggo2), are vulnerable to remote code execution due to missing integrity protection and validation of user-created programmes. The Android appl

9.1 **CVE-2026-27812** Sub2api sub2api

Sub2API is an AI API gateway platform designed to distribute and manage API quotas from AI product subscriptions. A vulnerability in versions prior to 0.1.85 is a Password Reset Poisoning (Host Header / Forwarded Header trust issue), which allows attackers to

9.1 **CVE-2026-27804** Parseplatform parse-server

Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 8.6.3 and 9.1.1-alpha.4, an unauthenticated attacker can forge a Google authentication token with `alg: "none"` to log in as any user link

Ransomware

No leak-site posts collected.

New data breaches 1

Odido odido.nl 6,077,025 accounts

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.