Daily brief, Monday, February 2, 2026

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

Generated Nov 7, 2026, 7:39 PM 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

9.8 **CVE-2026-22778** Vllm vllm DETECTION

vLLM is an inference and serving engine for large language models (LLMs). From 0.8.3 to before 0.14.1, when an invalid image is sent to vLLM's multimodal endpoint, PIL throws an error. vLLM returns this error to the client, leaking a heap address. With this le

9.1 **CVE-2026-25137**

The NixOs Odoo package is an open source ERP and CRM system. From 21.11 to before 25.11 and 26.05, every NixOS based Odoo setup publicly exposes the database manager without any authentication. This allows unauthorized actors to delete and download the entire

9.9 **CVE-2026-23515** Signalk signal k server

Signal K Server is a server application that runs on a central hub in a boat. Prior to 1.5.0, a command injection vulnerability allows authenticated users with write permissions to execute arbitrary shell commands on the Signal K server when the set-system-tim

9.8 **CVE-2025-66480** Wildfirechat im-server

Wildfire IM is an instant messaging and real-time audio/video solution. Prior to 1.4.3, a critical vulnerability exists in the im-server component related to the file upload functionality found in com.xiaoleilu.loServer.action.UploadFileAction. The application

10.0 **CVE-2026-25142** Nyariv sandboxjs

SandboxJS is a JavaScript sandboxing library. Prior to 0.8.27, SanboxJS does not properly restrict __lookupGetter__ which can be used to obtain prototypes, which can be used for escaping the sandbox / remote code execution. This vulnerability is fixed in 0.8.2

9.6 **CVE-2024-2356**

A Local File Inclusion (LFI) vulnerability exists in the '/reinstall_extension' endpoint of the parisneo/lollms-webui application, specifically within the `name` parameter of the `@router.post("/reinstall_extension")` route. This vulnerability allows attackers

9.1 **CVE-2024-5986**

A vulnerability in h2oai/h2o-3 version 3.46.0.1 allows remote attackers to write arbitrary data to any file on the server. This is achieved by exploiting the `/3/Parse` endpoint to inject attacker-controlled data as the header of an empty file, which is then e

9.8 **CVE-2022-50981**

An unauthenticated remote attacker can gain full access on the affected devices as they are shipped without a password by default and setting one is not enforced.

9.8 **CVE-2026-25200** Samsung magicinfo 9 server

A vulnerability in MagicInfo9 Server allows authorized users to upload HTML files without authentication, leading to Stored XSS, which can result in account takeover This issue affects MagicINFO 9 Server: less than 21.1090.1.

9.8 **CVE-2025-15030**

The User Profile Builder WordPress plugin before 3.15.2 does not have a proper password reset process, allowing a few unauthenticated requests to reset the password of any user by knowing their username, such as administrator ones, and therefore gain access to

9.8 **CVE-2026-25202** Samsung magicinfo 9 server

The database account and password are hardcoded, allowing login with the account to manipulate the database in MagicInfo9 Server.This issue affects MagicINFO 9 Server: less than 21.1090.1.

9.8 **CVE-2026-20418** Google matter

In Thread, there is a possible out of bounds write due to a missing bounds check. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00465153; Issue

9.3 **CVE-2026-24471**

continuwuity is a Matrix homeserver written in Rust. This vulnerability allows an attacker with a malicious remote server to cause the local server to sign an arbitrary event upon user interaction. Upon a user account leaving a room (rejecting an invite), join

9.3 **CVE-2026-20407** Mediatek nbiot sdk

In wlan STA driver, there is a possible escalation of privilege due to a missing bounds check. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00464377; Iss

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.