Daily brief, Saturday, February 14, 2026

Feb 13, 7:00 PM to Feb 14, 7:00 PM ET

Generated Nov 7, 2026, 5:26 PM ET

0	0	0	2	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

2 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

2

9.8 **CVE-2026-1306** DETECTION

The midi-Synth plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type and file extension validation in the 'export' AJAX action in all versions up to, and including, 1.1.0. This makes it possible for unauthenticated attackers to

9.8 **CVE-2025-8572**

The Truelysell Core plugin for WordPress is vulnerable to privilege escalation in versions less than, or equal to, 1.8.7. This is due to insufficient validation of the user_role parameter during user registration. This makes it possible for unauthenticated att

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.