Daily brief, Saturday, January 24, 2026

Jan 23, 7:00 PM to Jan 24, 7:00 PM ET

Generated Nov 7, 2026, 8:53 PM ET

0	0	0	7	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

7 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

7

9.8 **CVE-2026-22582** Salesforce marketing cloud engagement

+1 more CVEs in the same release

Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') vulnerability in Salesforce Marketing Cloud Engagement (MicrositeUrl module) allows Web Services Protocol Manipulation. This issue affects Marketing Cloud Engagement: before Jan

9.8 **CVE-2026-22586** Salesforce marketing cloud engagement

Hard-coded Cryptographic Key vulnerability in Salesforce Marketing Cloud Engagement (CloudPages, Forward to a Friend, Profile Center, Subscription Center, Unsub Center, View As Webpage modules) allows Web Services Protocol Manipulation. This issue affects Mark

9.8 **CVE-2026-22585** Salesforce marketing cloud engagement

Use of a Broken or Risky Cryptographic Algorithm vulnerability in Salesforce Marketing Cloud Engagement (CloudPages, Forward to a Friend, Profile Center, Subscription Center, Unsub Center, View As Webpage modules) allows Web Services Protocol Manipulation. Thi

9.8 **CVE-2025-13374**

The Kalrav AI Agent plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the kalrav_upload_file AJAX action in all versions up to, and including, 2.3.3. This makes it possible for unauthenticated attackers to uplo

9.8 **CVE-2025-13952** Imaginationtech ddk

A web page that contains unusual GPU shader code is loaded from the Internet into the GPU compiler process triggers a write use-after-free crash in the GPU shader compiler library. On certain platforms, when the compiler process has system privileges this coul

9.3 **CVE-2026-24399** Chattermate chattermate

ChatterMate is a no-code AI chatbot agent framework. In versions 1.0.8 and below, the chatbot accepts and executes malicious HTML/JavaScript payloads when supplied as chat input. Specifically, an <iframe> payload containing a javascript: URI can be processed a

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.