Daily brief, Friday, February 13, 2026

Feb 12, 7:00 PM to Feb 13, 7:00 PM ET

Generated Nov 7, 2026, 5:38 PM ET

0	1	0	9	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 9 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

9.9 **CVE-2026-1731** BeyondTrust Remote Support (RS) and Privileged Remote Ac… CISA KEV DETECTION

Unauthenticated remote attacker can execute OS commands as the site user in BeyondTrust Remote Support and Privileged Remote Access via OS command injection.

New public exploit code

No new Nuclei templates, Metasploit modules, Exploit-DB or VulnCheck XDB entries.

New critical CVEs

9

9.9 **CVE-2026-1731** BeyondTrust Remote Support (RS) and Privileged… KEV EXPLOIT CODE DETECTION

Unauthenticated remote attacker can execute OS commands as the site user in BeyondTrust Remote Support and Privileged Remote Access via OS command injection.

9.8 **CVE-2026-23112** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: nvmet-tcp: add bounds checks in nvmet_tcp_build_pdu_iovec nvmet_tcp_build_pdu_iovec() could walk past cmd->req.sg when a PDU length or offset exceeds sg_cnt and then use bogus sg->length/offse

9.8 **CVE-2026-26190** Milvus milvus DETECTION

Milvus is an open-source vector database built for generative AI applications. Prior to 2.5.27 and 2.6.10, Milvus exposes TCP port 9091 by default, which enables authentication bypasses. The /expr debug endpoint uses a weak, predictable default authentication

9.8 **CVE-2026-26335** Calero verasmart

Calero VeraSMART versions prior to 2022 R1 use static ASP.NET/IIS machineKey values configured for the VeraSMART web application and stored in C:\\Program Files (x86)\\Veramark\\VeraSMART\\WebRoot\\web.config. An attacker who obtains these keys can craft a val

9.8 **CVE-2026-26221**

Hyland OnBase contains an unauthenticated .NET Remoting exposure in the OnBase Workflow Timer Service (Hyland.Core.Workflow.NTService.exe). An attacker who can reach the service can send crafted .NET Remoting requests to default HTTP channel endpoints on TCP/8

9.8 **CVE-2026-26333** Calero verasmart

Calero VeraSMART versions prior to 2022 R1 expose an unauthenticated .NET Remoting HTTP service on TCP port 8001. The service publishes default ObjectURIs (including EndeavorServer.rem and RemoteFileReceiver.rem) and permits the use of SOAP and binary formatte

9.8 **CVE-2026-26273** Withknown known

Known is a social publishing platform. Prior to 1.6.3, a Critical Broken Authentication vulnerability exists in Known 1.6.2 and earlier. The application leaks the password reset token within a hidden HTML input field on the password reset page. This allows any

10.0 **CVE-2025-69770**

A zip slip vulnerability in the /DesignTools/SkinList.aspx endpoint of MojoPortal CMS v2.9.0.1 allows attackers to execute arbitrary commands via uploading a crafted zip file.

9.8 **CVE-2025-69633**

A SQL Injection vulnerability in the Advanced Popup Creator (advancedpopupcreator) module for PrestaShop 1.1.26 through 1.2.6 (Fixed in version 1.2.7) allows remote unauthenticated attackers to execute arbitrary SQL queries via the fromController parameter in

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.