Daily brief, Thursday, January 1, 2026

Dec 31, 7:00 PM to Jan 1, 7:00 PM ET

Generated Nov 9, 2026, 1:34 AM 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

9.6 **CVE-2025-66398** Signalk signal k server

Signal K Server is a server application that runs on a central hub in a boat. Prior to version 2.19.0, an unauthenticated attacker can pollute the internal state (`restoreFilePath`) of the server via the `/skServer/validateBackup` endpoint. This allows the att

9.1 **CVE-2025-68620** Signalk signal k server

Signal K Server is a server application that runs on a central hub in a boat. Versions prior to 2.19.0 expose two features that can be chained together to steal JWT authentication tokens without any prior authentication. The attack combines WebSocket-based req

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.