Daily brief, Sunday, November 30, 2025

Nov 29, 7:00 PM to Nov 30, 7:00 PM ET

Generated Nov 9, 2026, 6:43 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

9.1 **CVE-2025-35028**

By providing a command-line argument starting with a semi-colon ; to an API endpoint created by the EnhancedCommandExecutor class of the HexStrike AI MCP server, the resultant composed command is executed directly in the context of the MCP server’s normal priv

9.8 **CVE-2025-13615**

The StreamTube Core plugin for WordPress is vulnerable to Arbitrary User Password Change in versions up to, and including, 4.78. This is due to the plugin providing user-controlled access to objects, letting a user bypass authorization and access system resour

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.