Daily brief, Friday, November 28, 2025

Nov 27, 7:00 PM to Nov 28, 7:00 PM ET

Generated Nov 9, 2026, 7:01 AM ET

0	1	0	2	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 2 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

5.4 **CVE-2021-26829** OpenPLC ScadaBR CISA KEV

Cross-site scripting in OpenPLC ScadaBR via system_settings.shtm lets an attacker inject script that runs in the victim's browser session.

New public exploit code

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

New critical CVEs

2

9.4 **CVE-2025-66385**

UsersController::edit in Cerebrate before 1.30 allows an authenticated non-privileged user to escalate their privileges (e.g., obtain a higher role such as admin) via the user-edit endpoint by supplying or modifying role_id or organisation_id fields in the edi

9.3 **CVE-2025-64314** Huawei harmonyos

Permission control vulnerability in the memory management module. Impact: Successful exploitation of this vulnerability may affect confidentiality.

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.