Daily brief, Thursday, November 13, 2025

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

Generated Nov 9, 2026, 9:17 AM ET

0	0	0	7	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

7 new critical CVEs, 1 new breaches.

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

9.1 **CVE-2025-12762** Pgadmin pgadmin 4

pgAdmin versions up to 9.9 are affected by a Remote Code Execution (RCE) vulnerability that occurs when running in server mode and performing restores from PLAIN-format dump files. This issue allows attackers to inject and execute arbitrary commands on the ser

9.8 **CVE-2025-59367** Asus dsl-ac51 firmware

An authentication bypass vulnerability has been identified in certain DSL series routers, may allow remote attackers to gain unauthorized access into the affected system. Refer to the 'Security Update for DSL Series Router' section on the ASUS Security Advisor

10.0 **CVE-2025-36250** Ibm vios

IBM AIX 7.2, and 7.3 and IBM VIOS 3.1, and 4.1 NIM server (formerly known as NIM master) service (nimesis) could allow a remote attacker to execute arbitrary commands due to improper process controls. This addresses additional attack vectors for a vulnerabilit

9.6 **CVE-2025-36251** Ibm vios

IBM AIX 7.2, and 7.3 and IBM VIOS 3.1, and 4.1 nimsh service SSL/TLS implementations could allow a remote attacker to execute arbitrary commands due to improper process controls. This addresses additional attack vectors for a vulnerability that was previously

9.8 **CVE-2025-64717** Zitadel zitadel

ZITADEL is an open source identity management platform. Starting in version 2.50.0 and prior to versions 2.71.19, 3.4.4, and 4.6.6, a vulnerability in ZITADEL's federation process allowed auto-linking users from external identity providers to existing users in

9.6 **CVE-2025-64709** Typebot typebot

Typebot is an open-source chatbot builder. In versions prior to 3.13.1, a Server-Side Request Forgery (SSRF) vulnerability in the Typebot webhook block (HTTP Request component) functionality allows authenticated users to make arbitrary HTTP requests from the s

9.0 **CVE-2025-36096** Ibm vios

IBM AIX 7.2, and 7.3 and IBM VIOS 3.1, and 4.1 stores NIM private keys used in NIM environments in an insecure way which is susceptible to unauthorized access by an attacker using man in the middle techniques.

Ransomware

No leak-site posts collected.

New data breaches 1

Operation Endgame 3.0 2,046,030 accounts

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.