Daily brief, Monday, November 10, 2025

Nov 9, 7:00 PM to Nov 10, 7:00 PM ET

Generated Nov 9, 2026, 9:55 AM ET

0	1	0	6	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 6 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

8.8 **CVE-2025-21042** Samsung Mobile Devices CISA KEV

A remote attacker can execute arbitrary code on Samsung mobile devices through an out-of-bounds write in the libimagecodec.quram.so library.

New public exploit code

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

New critical CVEs

6

9.6 **CVE-2025-11892** GitHub enterprise server

An improper neutralization of input vulnerability was identified in GitHub Enterprise Server that allows DOM-based cross-site scripting via Issues search label filter that could lead to privilege escalation and unauthorized workflow triggers. Successful exploi

9.8 **CVE-2021-4462** Skittles employee records system DETECTION

Employee Records System version 1.0 contains an unrestricted file upload vulnerability that allows a remote unauthenticated attacker to upload arbitrary files via the uploadID.php endpoint; uploaded files can be executed because the application does not perfor

9.3 **CVE-2025-64513**

Milvus is an open-source vector database built for generative AI applications. An unauthenticated attacker can exploit a vulnerability in versions prior to 2.4.24, 2.5.21, and 2.6.5 to bypass all authentication mechanisms in the Milvus Proxy component, gaining

9.8 **CVE-2025-12866**

EIP Plus developed by Hundred Plus has a Weak Password Recovery Mechanism vulnerability, allowing unauthenticated remote attacker to predict or brute-force the 'forgot password' link, thereby successfully resetting any user's password.

9.8 **CVE-2025-12868**

New Site Server developed by CyberTutor has a Use of Client-Side Authentication vulnerability, allowing unauthenticated remote attackers to modify the frontend code to gain administrator privileges on the website.

9.1 **CVE-2025-64522** Charm soft serve

Soft Serve is a self-hostable Git server for the command line. Versions prior to 0.11.1 have a SSRF vulnerability where webhook URLs are not validated, allowing repository administrators to create webhooks targeting internal services, private networks, and clo

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.