Daily brief, Friday, November 14, 2025

Nov 13, 7:00 PM to Nov 14, 7:00 PM ET

Generated Nov 9, 2026, 9:07 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

9.4 **CVE-2025-64446** Fortinet FortiWeb CISA KEV DETECTION

Fortinet FortiWeb path traversal flaw lets an attacker gain unauthorized access to sensitive files and directories on the device.

New public exploit code

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

New critical CVEs

6

9.4 **CVE-2025-64446** Fortinet FortiWeb KEV EXPLOIT CODE DETECTION

Fortinet FortiWeb path traversal flaw lets an attacker gain unauthorized access to sensitive files and directories on the device.

9.8 **CVE-2025-13188** Dlink dir-816l firmware DETECTION

A vulnerability was detected in D-Link DIR-816L 2_06_b09_beta. Affected by this vulnerability is the function authenticationcgi_main of the file /authentication.cgi. Performing manipulation of the argument Password results in stack-based buffer overflow. Remot

9.3 **CVE-2021-4470**

TG8 Firewall contains a pre-authentication remote code execution vulnerability in the runphpcmd.php endpoint. The syscmd POST parameter is passed directly to a system command without validation and executed with root privileges. A remote, unauthenticated attac

9.8 **CVE-2025-13204** Silentmatt javascript expression evaluator

npm package `expr-eval` is vulnerable to Prototype Pollution. An attacker with access to express eval interface can use JavaScript prototype-based inheritance model to achieve arbitrary code execution. The npm expr-eval-fork package resolves this issue.

10.0 **CVE-2025-54339** Desktopalert pingalert application server

+1 more CVEs in the same release

An Incorrect Access Control vulnerability was found in the Application Server of Desktop Alert PingAlert version 6.1.0.11 to 6.1.1.2 exploitable remotely for Escalation of Privileges.

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.