

Daily brief, Thursday, October 15, 2026

Oct 14, 8:00 PM to Oct 15, 8:00 PM ET

Generated Oct 30, 2026, 2:41 AM ET

0

Breaking

0

Newly exploited

0

Exploit code

7

Critical CVEs

0

Ransomware posts

0

New breaches

7 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.

1 older CVE (published more than 7 days earlier) added to KEV, below the bar (CVSS under 9, not widely used enterprise tech):
[CVE-2026-21589 \(7.5\)](#)

New public exploit code

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

New critical CVEs

7

9.9

CVE-2026-110812 AWS Amazon Neptune Engine

An attacker gets arbitrary code execution in Amazon Neptune Engine with authentication.

9.6

CVE-2026-110916 Google Chrome

A remote attacker can execute arbitrary code outside the sandbox via a crafted HTML page in Google Chrome.

9.3

CVE-2026-99999 Linux Linux

A denial of service vulnerability exists in the Linux kernel due to an ipv4 checksum issue.

9.8

CVE-2026-98432 Linux Linux

An attacker can execute code with elevated privileges on Linux.

9.1

CVE-2026-55240 Msgbyte tianji

An attacker with a workspace admin account can inject malicious code into the Tianji platform.

9.2**CVE-2026-16436** Mitsubishi Electric GENESIS

An attacker can bypass authentication and access the Mitsubishi Electric GENESIS system.

9.4**CVE-2026-16438** Mitsubishi Electric GENESIS64

An attacker can escalate privileges in GENESIS64.

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. CVE IDs link to the full record on Watch Floor.