

Daily brief, Sunday, October 25, 2026

Oct 24, 8:00 PM to Oct 25, 8:00 PM ET

Generated Oct 29, 2026, 6:41 PM ET

2

Breaking

0

Newly exploited

1

Exploit code

2

Critical CVEs

21

Ransomware posts

0

New breaches

2 breaking, 2 emerging, 1 with new public exploit code, 2 new critical CVEs, 21 ransomware posts.

Breaking

2

PHP2Shell / HTTP2Shell · PHP

- 194 posts from 71 independent sources in 48 h
- PHP: very widely used in large enterprises
- remote code execution / auth bypass
- reports of exploitation in the wild
- public exploit code
- named threat actor activity

CVEs: [CVE-2026-111497](#), [CVE-2026-109618](#), [CVE-2026-109619](#), [CVE-2026-115560](#)

Arista Networks VeloCloud Orchestrator: SQL injection (2 CVEs)

- 17 posts from 12 independent sources in 48 h
- Arista / VeloCloud SD-WAN: widely used in large enterprises
- sql injection
- exploited in the wild (CISA KEV)
- official advisory

CVEs: [CVE-2026-114625](#), [CVE-2026-110447](#)

Emerging

2

Critical bugs in widely used enterprise tech, not spreading widely yet.

Oracle Java SE: Crypto / certificate

- 5 posts from 4 independent sources in 48 h
- rising: 5 posts in the last 24 h
- Java: very widely used in large enterprises
- remote code execution / auth bypass
- public exploit code
- official advisory

CVEs: [CVE-2026-114820](#)

Arm Mali Graphics Processing Unit (GPU): Memory corruption

- 6 posts from 4 independent sources in 48 h
- rising: 6 posts in the last 24 h
- Android: widely used in large enterprises
- exploited in the wild (CISA KEV)

CVEs: [CVE-2022-22706](#)

Newly exploited in the wild

No CVEs added to CISA's known-exploited list.

New public exploit code

1

5.9

CVE-2010-1428 Red Hat JBoss NUCLEI TEMPLATE KEV DETECTION

CVE published Apr 28, 2010

Unauthenticated access to the JBoss Application Server Web Console (/web-console) is blocked by default. However, it was found that this block was incomplete, and only blocked GET and POST HTTP verbs. A remote attacker could use this flaw to gain access to sen

New critical CVEs

2

9.1

CVE-2026-116207 YesWiki yeswiki

Product not on watchlist.

9.8

CVE-2026-115214 Unknown Datawiza Proxy Auth Plugin

An attacker can escalate privileges by creating a WordPress administrator account without authentication on Datawiza Proxy Auth Plugin.

Ransomware

21

21 victims posted to leak sites. Most active: NOn (6), qilin (5), emperador (3), Whitearmor (2), Falcon (2).

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.