

Daily brief, Friday, October 2, 2026

Oct 1, 8:00 PM to Oct 2, 8:00 PM ET

Generated Oct 31, 2026, 4:01 PM ET

0

Breaking

2

Newly exploited

0

Exploit code

3

Critical CVEs

0

Ransomware posts

0

New breaches

2 newly exploited, 3 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild2

- 8.7

CVE-2026-102489 Zammad Zammad

CISA KEV

An attacker gains remote code execution as the zammad user on Zammad.
- 8.5

CVE-2026-102490 Zammad Zammad

CISA KEV

The local zammad user can escalate privileges to root.

New public exploit code

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

New critical CVEs3

- 10.0

CVE-2026-103956 AWS loom

EXPLOIT CODE

DETECTION

An attacker can obtain super-admin authority without authentication on Loom for AWS.
- 9.0

CVE-2026-104019 AWS sagemaker-distribution

An attacker can inject OS commands into the Amazon SageMaker Distribution startup validation script.
- 9.9

CVE-2026-90970 GitLab GitLab AI Gateway

An attacker gets arbitrary code execution in GitLab AI Gateway.

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.