

Daily brief, Wednesday, September 16, 2026

Sep 15, 8:00 PM to Sep 16, 8:00 PM ET

Generated Nov 1, 2026, 5:41 AM ET

0

Breaking

3

Newly exploited

0

Exploit code

6

Critical CVEs

0

Ransomware posts

0

New breaches

3 newly exploited, 6 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

3

- 10.0

CVE-2026-76460 Cisco Identity Services Engine

CISA KEV

DETECTION

An unauthenticated attacker can bypass authentication and access a Cisco Identity Services Engine device.
- 8.8

CVE-2026-58704 Google Pixel

CISA KEV

An attacker can bypass authentication checks on a Google Pixel device and escalate privileges.
- 7.8

CVE-2026-87886 Acronis Backup

CISA KEV

An attacker can escalate privileges on Acronis Backup due to incorrect default permissions.

New public exploit code

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

New critical CVEs

6

- 10.0

CVE-2026-76460 Cisco Identity Services Engine

KEV

EXPLOIT CODE

DETECTION

An unauthenticated attacker can bypass authentication and access a Cisco Identity Services Engine device.
- 9.9

CVE-2026-20329 Cisco Cisco Secure Firewall Adaptive Security Appliance (ASA) Software

+3 more CVEs in the same release

An attacker can gain privilege escalation on a Cisco Secure Firewall Adaptive Security Appliance (ASA) Software server.
- 9.8

CVE-2025-56563

An unauthenticated remote attacker can make the Zenith Satellite Tracker make requests to arbitrary addresses.

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.