Daily brief, Wednesday, October 21, 2026

Oct 20, 8:00 PM to Oct 21, 8:00 PM ET

Generated Oct 29, 2026, 9:46 PM ET

0	0	0	26	37	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

26 new critical CVEs, 37 ransomware posts.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

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

New public exploit code

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

New critical CVEs

26

9.8 **CVE-2026-109618** PHP Group PHP KEV EXPLOIT CODE DETECTION

An attacker gains ability to execute arbitrary code by opening a malicious PHP script.

9.8 **CVE-2026-96639** Python pillow

An attacker can cause memory corruption of the Python imaging library.

9.8 **CVE-2026-76473** Cisco Cisco Emergency Responder

+2 more CVEs in the same release

An attacker can inject malicious code into affected Cisco products.

9.8 **CVE-2026-76466** Cisco Cisco TelePresence Video Communication Server (VCS) Expressway

An unauthenticated attacker can execute arbitrary operations on affected Cisco devices.

9.1 **CVE-2026-91403** Oracle Oracle Java SE

An attacker can bypass authentication and access Oracle Java SE.

9.0 **CVE-2026-20043** Cisco Cisco Cyber Vision

This vulnerability is related to memory corruption in Cisco Cyber Vision.

9.8 **CVE-2026-76301** Splunk Splunk Enterprise
An attacker gains data access to Splunk Enterprise without authentication or user interaction.

9.8 **CVE-2026-113736** D-Link DHP-W610AV
An attacker can set an empty password on D-Link DHP-W610AV.

10.0 **CVE-2026-105944** Apache Apache Pulsar Manager
An attacker can bypass authentication and access Pulsar Manager's user accounts.

10.0 **CVE-2026-114382** TOTOLINK EX200
An attacker can execute arbitrary code on a TOTOLINK EX200 by manipulating the argument of the setStaticDhcpConfig function.

10.0 **CVE-2026-113744** Tenda AC19
Product not on watchlist.

9.8 **CVE-2026-111183** GStreamer GStreamer
An attacker can execute arbitrary code on affected installations of GStreamer without authentication or user interaction.

9.1 **CVE-2026-114139** Getsentry sentry-javascript
An attacker can bypass application middleware for every request path under a configured tunnelRoute in Sentry-Javascript.

9.9 **CVE-2026-71195** OpenStack Manila
An attacker can bypass authentication and access public shares on OpenStack Manila before 23.0.1.

9.8 **CVE-2026-114119** Best Practice Software Bp Premier
An attacker can bypass authentication and access affected Bp Premier installations.

9.8 **CVE-2026-114108** HKUDS Vibe-Trading
An unauthenticated attacker can access the FastAPI surface of affected Vibe-Trading installations.

10.0 **CVE-2026-111813** Apache Apache Traffic Server
Apache Traffic Server's experimental magick plugin lets an unauthenticated client control ImageMagick convert arguments in its default (unsigned) configuration. This issue affects Apache Traffic Server: from 8.0.1 through 8.1.11, from 9.0.0 through 9.2.15, fro

9.4 **CVE-2026-113788** Uselagoon lagoon
An attacker can execute arbitrary code in lagoon.

10.0 **CVE-2026-111812** Apache Apache Traffic Server
Apache Traffic Server's origin_server_auth plugin lets a client force signing of attacker-chosen AWS request headers under the proxy's own credentials. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.11, from 9.0.0 through 9.2.15, from 10.0.0

9.0 **CVE-2026-111811** Apache Apache Traffic Server
An attacker can bypass authentication and read, write, and delete the shared proxy cache in Apache Traffic Server.

4 more critical CVEs in this window: see the dashboard

Ransomware 37

37 victims posted to leak sites. Most active: N0n (9), BrainCipher (8), lamashtu (3), everest (3), akira (2).

Financial services hit: Adobe Insurance Brokers, LLC (pear).

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.