

Daily brief, Saturday, October 24, 2026

Oct 23, 8:00 PM to Oct 24, 8:00 PM ET

Generated Oct 29, 2026, 7:19 PM ET

3

Breaking

0

Newly exploited

6

Exploit code

11

Critical CVEs

22

Ransomware posts

0

New breaches

3 breaking, 6 with new public exploit code, 11 new critical CVEs, 22 ransomware posts.

Breaking

3

PHP2Shell · PHP

- 121 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-2026-109618](#), [CVE-2026-109619](#), [CVE-2026-115560](#)

http2shell / Node2Shell · Node.js

- 49 posts from 20 independent sources in 48 h
- rising: 41 posts in the last 24 h
- Node.js: very widely used in large enterprises
- remote code execution / auth bypass
- public exploit code

CVEs: [CVE-2026-111497](#)

Arista Networks VeloCloud Orchestrator: SQL injection (2 CVEs)

- 16 posts from 13 independent sources in 48 h
- rising: 13 posts in the last 24 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](#)

Newly exploited in the wild

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

New public exploit code

6

10.0

CVE-2026-76460 Cisco Identity Services Engine

NUCLEI TEMPLATE

KEY

DETECTION

Known since Sep 16, 2026

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

9.8

CVE-2026-90817 Vanderbilt University REDCap

NUCLEI TEMPLATE

DETECTION

CVE published Sep 20, 2026

An attacker can execute arbitrary code on the server without authentication to the REDCap application.

9.8

CVE-2026-89079 Jfarthing84 Theme My Login

NUCLEI TEMPLATE

DETECTION

CVE published Oct 16, 2026

The Theme My Login plugin for WordPress is vulnerable to privilege escalation via account takeover in versions up to, and including, 7.2.1. This is due to the plugin not properly validating a user's identity prior to updating their password. This makes it poss

9.8

CVE-2026-89026 Issabel Foundation Issabel Framework

NUCLEI TEMPLATE

DETECTION

CVE published Sep 15, 2026

An attacker can forge valid bearer tokens without authentication to the Issabel Framework.

9.8

CVE-2026-82901 Themefic Ultra Addons for Contact Form 7

NUCLEI TEMPLATE

DETECTION

CVE published Sep 26, 2026

An attacker can upload arbitrary files without authentication to the Ultra Addons for Contact Form 7 plugin for WordPress.

9.3

CVE-2026-56062 Ooooogle Quotes llama

NUCLEI TEMPLATE

DETECTION

CVE published Jun 26, 2026

Unauthenticated SQL Injection in Quotes llama <= 3.1.5 versions.

2 older CVEs (published more than 7 days earlier) with new exploit code, below the bar (CVSS under 9, not widely used enterprise tech):

[CVE-2026-18110](#) (8.7), [CVE-2026-16535](#) (6.1)

New critical CVEs

11

9.1

CVE-2026-114820 Oracle Oracle Java SE

EXPLOIT CODE

Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u511-b32, 8u511-perf-b32, 11.0.33.0.2, 17.0.21.0.2, 21.0.13.0.

9.4

CVE-2026-115557 Python Software Foundation CPython

Compromised certificates are automatically rejected in CPython.

9.6	CVE-2026-115995 Unitree Robotics Unitree Go2 An attacker can execute arbitrary OS commands remotely on Unitree Go2.
9.8	CVE-2026-115806 Codexonics Prime Mover – Backup and Migration An attacker can inject objects via deserialization on Prime Mover – Backup and Migration.
9.8	CVE-2026-114196 Paytiumsupport Paytium An attacker can inject objects via deserialization on Paytium.
9.8	CVE-2026-94075 Tribulant Software Newsletters An attacker can inject objects via deserialization on Tribulant Software Newsletters.
9.6	CVE-2026-115932 GitroomHQ postiz-app A registered user can access arbitrary files on the server hosting postiz-app.
9.3	CVE-2026-111402 Tribulant Software Newsletters An attacker performs SQL Injection on Tribulant Software Newsletters.
9.3	CVE-2026-112866 WPFactory Product Filter by WBW An attacker performs Blind SQL Injection on WPFactory Product Filter by WBW.
9.9	CVE-2026-115933 GitroomHQ postiz-app An attacker can bypass authentication on postiz-app by using a shared secret.
9.8	CVE-2026-110956 Unknown asVereinbase An attacker can bypass authentication and log in as any user on asVereinbase.

Ransomware

22

22 victims posted to leak sites. Most active: krybit (6), N0n (5), thegentlemen (3), qilin (3), emperador (2).

Financial services hit: Commonwealth Community Bank (qilin).

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.