

Daily brief, Wednesday, October 28, 2026

Oct 27, 8:00 PM to Oct 28, 8:00 PM ET

Generated Oct 29, 2026, 3:21 PM ET

2

Breaking

2

Newly exploited

7

Exploit code

33

Critical CVEs

24

Ransomware posts

0

New breaches

2 breaking, 2 emerging, 2 newly exploited, 7 with new public exploit code, 33 new critical CVEs, 24 ransomware posts.

Breaking

2

PHP2Shell / Node2Shell · PHP

- 164 posts from 76 independent sources in 48 h
- PHP: very widely used in large enterprises
- remote code execution / auth bypass
- exploited in the wild (CISA KEV)
- public exploit code
- named threat actor activity

CVEs: [CVE-2026-111497](#), [CVE-2026-109618](#), [CVE-2026-109619](#), [CVE-2026-48356](#)

Apple Multiple Products: Memory corruption

- 8 posts from 7 independent sources in 48 h
- rising: 6 posts in the last 24 h
- macOS / iOS: very widely used in large enterprises
- remote code execution / auth bypass
- exploited in the wild (CISA KEV)
- emergency / unpatched

CVEs: [CVE-2026-86950](#)

Emerging

2

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

Oracle PeopleSoft Enterprise PeopleTools: Auth bypass / access control

- 5 posts from 5 independent sources in 48 h
- rising: 5 posts in the last 24 h
- Oracle: very widely used in large enterprises
- auth bypass / access control
- exploited in the wild (CISA KEV)
- public exploit code

CVEs: [CVE-2026-35273](#)

Arista Networks VeloCloud Orchestrator: SQL injection (2 CVEs)

- 6 posts from 4 independent sources in 48 h
- Arista / VeloCloud SD-WAN: widely used in large enterprises
- sql injection
- exploited in the wild (CISA KEV)

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

Newly exploited in the wild

2

7.8

CVE-2026-46300 Linux Linux CISA KEV**CVE published May 23, 2026**

In the Linux kernel, the following vulnerability has been resolved: net: skbuff: preserve shared-frag marker during coalescing skb_try_coalesce() can attach paged frags from @from to @to. If @from has SKBFL_SHARED_FRAG set, the resulting @to skb can contain th

2.7

CVE-2026-41709 VMware Cloud Foundation CISA KEV**CVE published Jul 30, 2026**

VMware ESX contains an insufficient logging vulnerability. A malicious administrator could exploit this issue to perform certain operations without them being logged.

New public exploit code

7

9.8

CVE-2026-116485 Huangxd- danmu api NUCLEI TEMPLATE DETECTION

Affected: danmu_api before 1.21.7. Attacker gains: Ability to modify server environment configuration. Recommended action: Update danmu_api to version 1.21.7 or later.

5.3

CVE-2026-116205 YesWiki yeswiki NUCLEI TEMPLATE DETECTION

YesWiki before 4.7.0 contains an unauthenticated server-side request forgery vulnerability that allows remote attackers to fetch arbitrary URLs by supplying [[[URL]]] wiki syntax to the render handler. Attackers can pass the syntax in the content parameter of t

10.0

CVE-2026-105134 Ahsay AhsayCBS

NUCLEI TEMPLATE

KEV

DETECTION

CVE published Oct 4, 2026

An attacker can execute arbitrary OS commands on AhsayCBS.

10.0

CVE-2026-24898 Openemr openemr

NUCLEI TEMPLATE

DETECTION

CVE published Mar 3, 2026

Affected: OpenEMR prior to version 8.0.0. Attacker gains: Unauthenticated MedEx API tokens. Recommended action: Update OpenEMR to version 8.0.0 or later.

10.0

CVE-2026-18051 Unknown W3 Total Cache

NUCLEI TEMPLATE

DETECTION

CVE published Aug 19, 2026

The W3 Total Cache WordPress plugin before 2.10.5 does not properly validate the request path it uses to build cache file names, allowing unauthenticated attackers to write a file into any existing directory on the server, inside or outside the web root, overw

9.8

CVE-2026-76443 Cisco Cisco Secure Email

METASPLOIT MODULE

CVE published Sep 14, 2026

Product not on watchlist.

9.3

CVE-2026-85595 Traefik traefik

NUCLEI TEMPLATE

DETECTION

CVE published Sep 4, 2026

(1) Traefik versions before v2.11.55 and versions v3.0.0 through v3.7.10. (2) An attacker gains the ability to compute a valid digest response, potentially bypassing authentication. (3) Upgrade to Traefik v2.11.55 or later, or v3.7.11 or later.

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

[CVE-2026-108123 \(7.5\)](#)

New critical CVEs

33

9.8

CVE-2026-103406 Juniper Networks Session Smart Conductor

Product not on watchlist.

9.8

CVE-2026-103409 Juniper Networks Session Smart Router

Product not on watchlist.

9.8

CVE-2026-110879 FasterXML jackson-databind

An attacker can gain remote code execution on a server using jackson-databind.

9.8

CVE-2026-86400 Dell PowerProtect Data Domain**+3 more CVEs in the same release**

An attacker can bypass authentication in Dell PowerProtect Data Domain without authentication.

9.9

CVE-2026-44179 Xwikisas xwiki-pro-macros

XWiki Remote Macros provides XWiki rendering macros that are useful when migrating content from Confluence. From 1.13 until 1.14.5, the `excerpt-include` macro does not properly escape the included page's title and executes `excerpt` content with the macro's r

9.8

CVE-2026-109218 Kleor Contact Manager

An attacker can upload arbitrary files to the Contact Manager plugin for WordPress.

9.8

CVE-2026-106013 Artbees Jupiter X Core

An attacker can bypass authentication for WordPress sites using the Jupiter X Core plugin.

9.4

CVE-2026-63190 Fearlessgeekmedia FearlessCMS

FearlessCMS is a flat-file `content` management system centered on simplicity and open source. Prior to version 0.1.4, five debug/test PHP scripts under `admin/` perform privileged operations without `isLoggedIn()` authentication checks, CSRF protection or ade

9.8

CVE-2026-84999 Pie Register Pie Register Premium

A remote attacker can upload arbitrary files via the piereg_file_upload function.

9.1

CVE-2026-14571 Futurum Software Futurum Software User Authentication Module

An attacker can inject malicious SQL queries in Futurum Software's management software.

9.4

CVE-2026-104383 EagleCloud Aquila

An authenticated remote attacker can execute arbitrary code in Aquila.

9.8

CVE-2026-103688 Unknown Checkout Files Upload for WooCommerce

An attacker can upload arbitrary files, including PHP files, without authentication.

9.6

CVE-2026-90717 Dell PowerProtect Data Domain Management Center

+2 more CVEs in the same release

An attacker can bypass authentication and access the Dell PowerProtect Data Domain Management Center.

10.0

CVE-2026-61564 WWBN AVideo-Encoder

An attacker can inject code on AVideo-Encoder via the installer endpoint.

10.0

CVE-2026-61567 WWBN AVideo-Encoder

An unauthenticated attacker can inject code on AVideo-Encoder via the live-streaming endpoint.

9.8

CVE-2026-118477 EISGE Kalifast

An authenticated attacker can execute arbitrary commands on KaliFast with www-data privileges.

9.8

CVE-2026-114278 Eclipse Foundation Eclipse Che

An attacker can inject code in Eclipse Che, affecting Eclipse Che with user interaction.

9.8

CVE-2026-115968 Ultimate Member Ultimate Member

An attacker can inject objects in Ultimate Member, affecting Ultimate Member.

9.8

CVE-2026-118690 SignalK signalk-server

An attacker can download log archives and extract the JWT secret key from Signal K Server without authentication.

9.8

CVE-2026-118579 D-Link DIR-505

An attacker can execute arbitrary code on D-Link DIR-505 remotely without authentication.

8 more critical CVEs in this window: [see the dashboard](#)

Ransomware

24

24 victims posted to leak sites. Most active: SilentRansomGroup (5), akira (3), Whitearmor (3), rhysida (2), payload (2).

Financial services hit: Insurance Services (akira).

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.