

Daily brief: the last 24 hours

Oct 28, 2:21 PM to Oct 29, 2:21 PM ET

Generated Oct 29, 2026, 2:21 PM ET

3

Breaking

0

Newly exploited

6

Exploit code

15

Critical CVEs

20

Ransomware posts

0

New breaches

3 breaking, 5 emerging, 6 with new public exploit code, 15 new critical CVEs, 20 ransomware posts.

Breaking

3

PHP2Shell · PHP

- 138 posts from 65 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-2026-41709](#), [CVE-2026-109619](#), [CVE-2026-48356](#), [CVE-2026-46300](#)

Cisco

- 14 posts from 14 independent sources in 48 h
- rising: 13 posts in the last 24 h
- Cisco: very widely used in large enterprises
- remote code execution / auth bypass
- reports of exploitation in the wild
- official advisory

CVEs: [CVE-2026-76418](#)

GitLab: Memory corruption

- 34 posts from 9 independent sources in 48 h
- rising: 34 posts in the last 24 h
- GitLab / GitHub: very widely used in large enterprises
- remote code execution / auth bypass
- public exploit code

CVEs: [CVE-2026-97229](#)

Emerging

5

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

Cisco Catalyst SD-WAN Controller and Manager: Auth bypass / access control

- 4 posts from 4 independent sources in 48 h
- Cisco: very widely used in large enterprises
- auth bypass / access control
- exploited in the wild (CISA KEV)
- public exploit code
- named threat actor activity

CVEs: [CVE-2026-20127](#)

Oracle PeopleSoft Enterprise PeopleTools: Auth bypass / access control

- 5 posts from 5 independent sources in 48 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](#)

Oracle Application Object Library: Auth bypass / access control

- 11 posts from 11 independent sources in 48 h
- Oracle: very widely used in large enterprises
- auth bypass / access control

CVEs: [CVE-2026-101767](#)

Linux

- 5 posts from 5 independent sources in 48 h
- rising: 5 posts in the last 24 h
- Linux kernel: very widely used in large enterprises
- remote code execution / auth bypass

CVEs: [CVE-2026-98432](#)

Apple Multiple Products: Memory corruption

- 3 posts from 3 independent sources in 48 h
- macOS / iOS: very widely used in large enterprises
- exploited in the wild (CISA KEV)

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

Newly exploited in the wild

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

New public exploit code

6

6.8

CVE-2026-116167 Siyuan-Note siyuan NUCLEI TEMPLATE DETECTION

SiYuan from 2.9.0 before 3.8.7 contains a cross-site scripting vulnerability in the unauthenticated /check-auth page that assigns the to parameter to window.location.href without scheme validation. Attackers can send a crafted link with a javascript: URI that

6.5

CVE-2026-116070 Dqzboy Docker-Proxy NUCLEI TEMPLATE DETECTION

Docker-Proxy through 5.1.9 contains a missing authentication vulnerability in the hubcmdui routes/config.js that allows unauthenticated attackers to read and overwrite configuration via /api/config. Attackers can retrieve the WeChat webhook URL and Telegram bo

6.5

CVE-2026-115886 pip mlflow NUCLEI TEMPLATE DETECTION

Summary MLflow's tracking server exposes `POST /ajax-api/3.0/mlflow/scorer/invoke` with ****no authentication****, and the handler reflectively instantiates an attacker-named class from attacker-supplied JSON with unconstrained constructor kwargs. With the opt

9.8

CVE-2026-110447 Collabora Collabora Online - Built-in CODE S... NUCLEI TEMPLATE KEV DETECTION

CVE published Oct 14, 2026

An attacker can execute remote code.

9.8

CVE-2026-104736 Thimpress LearnPress – WordPress LMS Plugin for... NUCLEI TEMPLATE DETECTION

CVE published Oct 17, 2026

An attacker gains arbitrary code execution on WordPress installations using LearnPress plugin versions up to 4.4.10.

9.8

CVE-2025-58434 FlowiseAI Flowise METASPLOIT MODULE DETECTION

CVE published Sep 12, 2025

Flowise is a drag & drop user interface to build a customized large language model flow. In version 3.0.5 and earlier, the `forgot-password` endpoint in Flowise returns sensitive information including a valid password reset `tempToken` without authentication o

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-2026-55864 \(7.8\)](#), [CVE-2026-48048 \(7.5\)](#)

New critical CVEs

15

-
- 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
-
- 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-2026-93680** IBM Langflow OSS
Product not on watchlist.
-
- 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.
-
- 9.8** **CVE-2026-109516** Guruteam Bot for Telegram on WooCommerce
An attacker can bypass authentication and take over accounts on the Bot for Telegram on WooCommerce plugin for WordPress.
-
- 9.8** **CVE-2026-42922** Frangoteam Frangoteam
Product not on watchlist.
-
- 9.8** **CVE-2026-97854** Yamaha NWR100
Yamaha wireless LAN router NWR100 provided by Yamaha Corporation contains an OS command injection vulnerability. Arbitrary OS commands may be executed by sending a specially crafted request to the affected product.
-
- 9.4** **CVE-2026-66088** Apereo Foundation openEQUELLA
An attacker gets remote code execution in openEQUELLA without authentication or user interaction.
-
- 9.3** **CVE-2026-114358** Radius Synergies Radius Xenia M2M Platform
This vulnerability exists in the Radius Xenia M2M Platform due to insufficient validation of user supplied input in the password recovery functionality in the web management interface. An unauthenticated remote attacker could exploit this vulnerability by supp
-
- 9.3** **CVE-2026-111732** RT-Labs P-Net
P-Net before 1.0.3, when built with PNET_OPTION_AR_VENDOR_BLOCKS enabled, parses a data length from a field of the ARVendorBlock request that is not part of the block definition and uses it as the number of bytes to copy into a fixed-size buffer, without compa
-

9.2

CVE-2026-112256 OpenText Advanced Authentication Server

Acceptance of extraneous untrusted data with trusted data vulnerability in OpenText Advanced Authentication Server allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Advanced Authentication Server: from 6.4.0.0 through 6.4.3.8,

9.1

CVE-2026-117574 Red Hat Red Hat OpenShift AI (RHOAI)

An authenticated attacker can access another tenant's model identifier, in Red Hat OpenShift AI.

9.1

CVE-2026-118264 Labstack echo

An attacker gets remote code execution in echo without authentication or user interaction.

Ransomware

20

20 victims posted to leak sites. Most active: Booba Project (6), SilentRansomGroup (4), lockbit5 (2), rhysida (1), pear (1).

Financial services hit: National Association of Credit Management (Booba Project), ClaimTek Systems (rhysida), xspringcapital.com (lockbit5).

New data breaches

No new breaches published.