Daily brief, Thursday, October 29, 2026

Oct 28, 8:00 PM to Oct 29, 8:00 PM ET

Generated Nov 6, 2026, 11:01 PM ET

5	2	6	85	29	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

5 breaking, 3 emerging, 2 newly exploited, 6 with new public exploit code, 85 new critical CVEs, 29 ransomware posts.

Breaking 5

PHP2Shell · PHP

- 104 posts from 52 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-2026-109618, CVE-2026-109619, CVE-2026-41709, CVE-2026-46300

Node2Shell / HTTP2Shell · Node.js

- 34 posts from 27 independent sources in 48 h
- Node.js: 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-2026-48356

Oracle PeopleSoft Enterprise PeopleTools: Auth bypass / access control

- 7 posts from 7 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

GitLab: Memory corruption

- 30 posts from 7 independent sources in 48 h
- rising: 30 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

Oracle Application Object Library: Auth bypass / access control

- 11 posts from 11 independent sources in 48 h
- rising: 9 posts in the last 24 h
- Oracle: very widely used in large enterprises
- auth bypass / access control

CVEs: CVE-2026-101767

Emerging 3

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

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

- 3 posts from 3 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
- official advisory

CVEs: CVE-2026-20127

Apple Multiple Products: Memory corruption

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

CVEs: CVE-2026-86950

Arista Networks VeloCloud Orchestrator: SQL injection

- 3 posts from 3 independent sources in 48 h
- Arista / VeloCloud SD-WAN: widely used in large enterprises
- exploited in the wild (CISA KEV)

CVEs: CVE-2026-114625

Newly exploited in the wild 2

8.6 **CVE-2026-76418** Cisco Secure Firewall ASA Software and Cisco Secure FTD Software CISA KEV

Unauthenticated remote attacker can reload Cisco Secure Firewall ASA and FTD devices via the Remote Access SSL VPN service, causing denial of service.

10.0 **CVE-2026-97229** GitLab GitLab CISA KEV DETECTION

CVE published Oct 13, 2026

An attacker can execute arbitrary code on the GitLab server without authentication.

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

Remote code execution via OS command injection in proxy.php of Collabora Online Built-in CODE Server (richdocumentscode Nextcloud app) before 26.4.303.

9.8 **CVE-2026-104736** Thimpress LearnPress – WordPress LMS Plugin for… NUCLEI TEMPLATE DETECTION

CVE published Oct 17, 2026

LearnPress WordPress LMS plugin through 4.4.10: PHP object injection via untrusted 'checkout-email' parameter gives attacker arbitrary code execution.

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 85

9.8 **CVE-2026-93680** IBM Langflow OSS EXPLOIT CODE

A remote attacker can bypass security restrictions in IBM Langflow OSS versions 1.0.0 through 1.12.8 due to improper authentication.

9.9 **CVE-2026-107328** IBM Langflow OSS EXPLOIT CODE

+1 more CVEs in the same release

A remote authenticated attacker can execute arbitrary code in IBM Langflow OSS versions 1.0.0 through 1.12.4 via unsanitized input passed to eval/exec.

9.9 **CVE-2026-107327** IBM Langflow OSS EXPLOIT CODE

A remote authenticated attacker can execute arbitrary code in IBM Langflow OSS 1.0.0 through 1.12.4 due to missing authorization checks.

10.0 **CVE-2026-84295** Progress Software WS FTP Server EXPLOIT CODE

Unauthenticated remote attackers can access sensitive information, including administrative credentials, in Progress WS_FTP Server before 2024.0.6 and 2025.0.3 on Windows.

9.4 **CVE-2026-103093** ServiceNow ServiceNow AI Platform

Authenticated users with the admin role can escape the Rhino sandbox in ServiceNow AI Platform to run arbitrary code on the host operating system.

9.8 **CVE-2026-61992** Von Eyal Fitoussi GEO my WordPress

An unauthenticated attacker can inject PHP objects through unsafe deserialization in GEO my WordPress versions up to and including 4.5.5.3.

9.9 **CVE-2026-90868** Progress Software WS FTP Server

+1 more CVEs in the same release

OS command injection in Progress WS_FTP Server before 2024.0.7 and 2025.0.4 on Windows lets an attacker run arbitrary commands in certain configurations.

9.8 **CVE-2026-97854** Yamaha NWR100

An attacker can execute arbitrary OS commands on the Yamaha NWR100 wireless LAN router by sending a specially crafted request.

9.9 **CVE-2026-119145** Frappe frappe

Authenticated attackers can upload crafted files to write outside the intended storage directory in Frappe before 15.121.0 and 16.x before 16.34.0.

10.0 **CVE-2026-61991** Ajax Load More AjaxLoadMore Cache

Unauthenticated remote code execution in AjaxLoadMore Cache versions 3.1.1 and earlier, a WordPress plugin, via code injection (CWE-94).

9.8 **CVE-2026-104339** IBM Langflow OSS

Remote attacker executes arbitrary code in IBM Langflow OSS 1.0.0 through 1.12.3 via OS command injection.

9.1 **CVE-2026-90866** Progress Software WS FTP Server

+1 more CVEs in the same release

An attacker gets data access with Progress Software WS FTP Server without authentication.

9.4 **CVE-2026-66088** Apereo Foundation openEQUELLA

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

9.1 **CVE-2026-90863** Progress Software WS FTP Server

An attacker gets privilege escalation with Progress Software WS FTP Server without authentication.

9.8 **CVE-2026-110186** IBM Langflow OSS

A remote attacker gets arbitrary code execution in IBM Langflow OSS versions 1.0.0 through 1.12.8 through improper control of code generation (CWE-94).

9.8 **CVE-2026-109516** Guruteam Bot for Telegram on WooCommerce

Authentication bypass in the Bot for Telegram on WooCommerce WordPress plugin through 1.3.0 lets an attacker take over user accounts via its woo-telegram REST endpoint.

9.8 **CVE-2026-42922** Frangoteam Frangoteam

An authorization bypass in the /nodered feature of Frangoteam FUXA 1.3.2-2809 lets a specially crafted HTTP request lead to arbitrary code execution.

9.8 **CVE-2026-54859** ThemeREX Preservation

Unauthenticated PHP object injection in ThemeREX Preservation theme up to 1.15 lets an attacker inject crafted PHP objects via unsafe deserialization.

9.3 **CVE-2023-22793** Microsoft Management Pack for Microsoft System Center

An attacker can execute code on servers running Veeam Management Pack for Microsoft System Center without authentication.

9.8 **CVE-2026-61997** ThemeREX Legal Stone

Unauthenticated PHP object injection in ThemeREX Legal Stone theme version 1.2.11 and earlier lets an attacker inject serialized PHP objects without logging in.

62 more critical CVEs in this window: see the dashboard

Ransomware 29

29 victims posted to leak sites. Most active: booba team (7), qilin (4), everstake (4), rhysida (2), global secret group (2).

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. Leak-site data: RansomLook (ransomlook.io), CC BY 4.0; sectors grouped and countries mapped by Watch Floor. CVE IDs link to the full record on Watch Floor.