Daily brief, Friday, October 30, 2026

Oct 29, 8:00 PM to Oct 30, 8:00 PM ET

Generated Nov 6, 2026, 8:56 PM ET

4	2	3	49	43	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

4 breaking, 3 emerging, 2 newly exploited, 3 with new public exploit code, 49 new critical CVEs, 43 ransomware posts.

Breaking 4

PHP2Shell · PHP

- 177 posts from 72 independent sources in 48 h
- rising: 127 posts in the last 24 h
- PHP: very widely used in large enterprises
- remote code execution / auth bypass
- exploited in the wild (CISA KEV)
- public exploit code

CVEs: CVE-2026-98432, CVE-2026-109618, CVE-2026-41709, CVE-2026-111497, CVE-2026-109619, CVE-2026-46300

Cisco Secure Firewall ASA Software and Cisco Secure FTD Software

- 18 posts from 18 independent sources in 48 h
- rising: 12 posts in the last 24 h
- Cisco: very widely used in large enterprises
- remote code execution / auth bypass
- exploited in the wild (CISA KEV)
- official advisory

CVEs: CVE-2026-76418

GitLab: Memory corruption

- 42 posts from 16 independent sources in 48 h
- GitLab / GitHub: very widely used in large enterprises
- remote code execution / auth bypass
- exploited in the wild (CISA KEV)
- public exploit code
- official advisory

CVEs: CVE-2026-97229

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

- 7 posts from 6 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

Emerging 3

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

Ivanti Connect Secure: Privilege escalation (2 CVEs)

- 4 posts from 4 independent sources in 48 h
- Ivanti: very widely used in large enterprises
- privilege escalation
- exploited in the wild (CISA KEV)
- public exploit code
- official advisory

CVEs: CVE-2026-111357, CVE-2026-104935

Oracle Application Object Library: Auth bypass / access control

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

CVEs: CVE-2026-101767

Arista Networks VeloCloud Orchestrator: SQL injection

- 4 posts from 4 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

4.3 **CVE-2026-118527** Ivanti Connect Secure CISA KEV

A remote authenticated attacker can upload files with attacker-controlled content to a known on-disk location in Ivanti Connect Secure before 25.1.1.3 and 22.8R2.6, via predictable filenames.

7.0 **CVE-2026-111357** Ivanti Connect Secure CISA KEV

CVE published Oct 15, 2026

Attacker escalates to root on Ivanti Connect Secure 22.8R2.4 by abusing the dsinvoked broker's trust of DSCache configuration data; exploited in the wild.

New public exploit code 3

8.8 **CVE-2026-116748** Transmission transmission NUCLEI TEMPLATE DETECTION

A malicious web page can issue RPC calls on Transmission transmission without authentication.

9.8 **CVE-2023-54335** Extplorer eXtplorer NUCLEI TEMPLATE DETECTION

CVE published Jan 13, 2026

Affected: eXtplorer 2.1.14 (PHP-based web file manager) login/authentication logic. Attacker gains: unauthenticated login without a password, then can upload PHP files and achieve remote code execution, with full control of the hosting web server's files and d

9.8 **CVE-2023-31719** Frangoteam fuxa NUCLEI TEMPLATE DETECTION

CVE published Sep 21, 2023

FUXA <= 1.1.12 is vulnerable to SQL Injection via /api/signin.

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-2026-34151 (8.2), CVE-2026-14554 (6.5)

New critical CVEs 49

9.8 **CVE-2026-103039** Gravity Forms Gravity Forms EXPLOIT CODE

Gravity Forms through 3.1.2 allows PHP object injection via the List input type of Post Custom Fields, which unserializes submitted values without restriction.

9.5 **CVE-2026-116366** ClickHouse ClickHouse EXPLOIT CODE DETECTION
An attacker can execute arbitrary code on the ClickHouse Server without authentication.

10.0 **CVE-2026-112816** Canonical LXD EXPLOIT CODE
Canonical LXD HTTPS listener flaw lets an unauthenticated attacker authenticate as any trusted client via a crafted certificate, gaining full cluster and managed VM access.

9.8 **CVE-2026-63377** Fctr-Id okta-ai-agent
Unauthenticated network attacker can create the first admin account in TAKO AI Agent for Okta before 3.0.1-beta via /api/auth/setup.

9.4 **CVE-2026-93327** Google Cloud Application Integration
Authenticated attacker can run arbitrary code in Google Cloud Application Integration before 2026-09-11 via a crafted serialized object in SubWorkflow.

9.6 **CVE-2026-119261** Google Chrome
An attacker gets remote code execution on Chrome.

9.6 **CVE-2026-119263** Google Chrome
An attacker gets remote code execution on Chrome.

9.8 **ISSUE-GHSA4xm8rg9hjhq2** npm signalk-server
An attacker can read and write arbitrary files and execute remote code on the signalk-server.

9.8 **ISSUE-GHSAhff95pqw6w9f** go github.com/imgproxy/imgproxy/v3
A crafted ICO image triggers an integer overflow and heap memory corruption in the ICO loader of imgproxy v3 (Go), causing denial of service.

9.5 **ISSUE-GHSA5xjx3w67w9x9** actions pypa/gh-action-pypi-publish
An attacker can bypass certificate validation in the Sigstore used by PyPI.

9.8 **CVE-2025-31704** Dahua Intelligent Connection Center
A remote attacker sends a specially crafted request to Dahua Intelligent Connection Center to execute arbitrary commands, achieving remote code execution.

9.8 **CVE-2026-119706** InternLM lmdeploy
Unauthenticated remote attackers can run OS commands in InternLM LMDeploy 0.9.0 through 0.18.0 by sending a crafted pickle to the /update_weights endpoint.

9.8 **CVE-2026-110799** Givanz Vvveb
+1 more CVEs in the same release
Authentication bypass in the Vvveb CMS password reset function before 1.0.8.7, caused by insufficient validation of the user and token GET parameters.

9.1 **CVE-2026-116852** Marketing Fire Widget Options
An attacker gets remote code execution in Marketing Fire's Widget Options <= 4.2.5 versions.

9.8 **CVE-2026-78403** Thalesgroup Sentinel Keys Server
A crafted HTTP request with an overlong first field overflows a stack buffer in Thales Sentinel Keys Server on Windows, and the server also lacks an authorization check.

10.0 **CVE-2026-61738** Socfortress CoPilot
Path traversal in SOCFortress CoPilot's ScoutSuite GCP report endpoint lets authenticated admin or analyst users access files outside intended paths.

9.8 **CVE-2026-114523** Drupal Ffmpeg Image Toolkit
Attackers can inject OS commands into Drupal Ffmpeg Image Toolkit versions 0.0.0 through 1.0.3, executing arbitrary commands on the host.

9.8 **CVE-2026-119660** Yincongcyincong MuseBot
Unauthenticated attackers can forge admin sessions in MuseBot before 2.0.0 using a hard-coded default session key, gaining full administrative access.

9.8 **CVE-2026-61737** Huajian123 ng-antd-admin
Attackers forge JWTs with ng-antd-admin's hardcoded default secret in deployments that never changed it, bypassing authentication and impersonating any user.

9.1 **CVE-2026-62849** Mqttsnet thinglinks
An attacker can inject malicious SQL code in ThingLinks, allowing remote unauthenticated access.

28 more critical CVEs in this window: see the dashboard

Ransomware 43

43 victims posted to leak sites. Most active: qilin (11), genesis (9), leakeddata (4), the gentlemen (3), akira (3).

Financial services hit: iFink (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. 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.