

Daily brief, Tuesday, October 27, 2026

Oct 26, 8:00 PM to Oct 27, 8:00 PM ET

Generated Oct 29, 2026, 5:08 PM ET

2

Breaking

2

Newly exploited

6

Exploit code

47

Critical CVEs

43

Ransomware posts

1

New breaches

2 breaking, 2 newly exploited, 6 with new public exploit code, 47 new critical CVEs, 43 ransomware posts, 1 new breaches.

Breaking

2

PHP2Shell / Node2Shell · PHP

- 173 posts from 75 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-2026-111497](#), [CVE-2026-109619](#)

Arista Networks VeloCloud Orchestrator: SQL injection (2 CVEs)

- 8 posts from 6 independent sources in 48 h
- rising: 6 posts in the last 24 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

9.2

CVE-2026-111497 Google Brotli CISA KEV

A buffer overflow vulnerability in the Brotli decoder (c/dec/decode.c) in Google Brotli versions 1.0.3 through 1.2.0 on all platforms allows a remote unauthenticated attacker to corrupt adjacent decoder state memory, disclose sensitive memory contents, cause a

9.3

CVE-2026-48356 Adobe Adobe Commerce CISA KEY**CVE published Jul 14, 2026**

Adobe Commerce is affected by an Unrestricted Upload of File with Dangerous Type vulnerability that could result in arbitrary code execution in the context of the current user, potentially gaining elevated access or control over the victim's account or session

New public exploit code

6

8.2

CVE-2026-116067 Ananthakumaran paisa NUCLEI TEMPLATE DETECTION

Paisa before 0.7.8 contains a path traversal vulnerability in the GetFile, GetSheet, DeleteBackups, and DeleteSheetBackups handlers that lets unauthenticated attackers read files and delete backups through ../ sequences in file names. Attackers can send crafted

7.3

CVE-2026-116006 YunaiV ruoyi-vue-pro NUCLEI TEMPLATE DETECTION

A vulnerability was detected in YunaiV/zhijiantianya ruoyi-vue-pro up to 2026.09. The affected element is an unknown function of the file AuthController.java of the component SMS Code Verification. The manipulation of the argument mobile/code results in improp

10.0

CVE-2026-97359 Rejetto hfs2 NUCLEI TEMPLATE DETECTION**CVE published Sep 24, 2026**

An attacker can execute code without authentication on HFS2.

10.0

CVE-2024-56829 NUCLEI TEMPLATE DETECTION**CVE published Jan 2, 2025**

Huang Yaoshi Pharmaceutical Management Software through 16.0 allows arbitrary file upload via a .asp filename in the fileName element of the UploadFile element in a SOAP request to /XSDService.asmx.

7.1

CVE-2026-93485 Automattic WordPress NUCLEI TEMPLATE DETECTION**CVE published Sep 18, 2026**

Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Automattic WordPress wordpress allows DOM-Based XSS. This issue affects WordPress: from n/a through 7.1.

3.4

CVE-2026-9062 Unknown Store Locator WordPress NUCLEI TEMPLATE DETECTION**CVE published Jun 13, 2026**

The Store Locator WordPress plugin before 1.6.9 does not validate a parameter before using it in a file path, allowing high-privileged users such as administrators to read arbitrary .php files from the server, including configuration files that contain datab

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

[CVE-2026-17540](#) (8.8), [CVE-2026-11565](#) (8.5), [CVE-2026-9848](#) (7.5), [CVE-2026-16959](#) (6.8), [CVE-2026-10525](#) (6.1)

New critical CVEs

47

9.1

CVE-2026-114607 npm better-auth

An attacker can sign in as another user in better-auth.

-
- 9.1** **CVE-2026-108142** Veeam Backup & Replication
An unauthenticated attacker can bypass authorization on the Veeam Backup & Replication CDP Coordinator Service.
-
- 9.0** **CVE-2026-106076** Microsoft Backup for Microsoft 365
An attacker with organization-transfer peer access can inject SQL into the Veeam Backup for Microsoft 365 server, leading to cross-tenant data access and remote code execution.
-
- 9.6** **CVE-2026-118355** Google chrome
Improper input validation in Command in Google Chrome prior to 156.0.8078.73 allowed a remote attacker to potentially execute arbitrary code outside the sandbox via a crafted HTML page. (Chromium security severity: High)
-
- 9.6** **CVE-2026-118305** Google Chrome
An attacker can execute arbitrary code outside the sandbox via a crafted HTML page in Google Chrome.
-
- 9.6** **CVE-2026-118306** Google Chrome
A remote attacker can execute arbitrary code outside the sandbox via a crafted HTML page in Google Chrome.
-
- 9.6** **CVE-2026-118308** Google Chrome
A remote attacker can execute arbitrary code outside the sandbox via a crafted HTML page in Google Chrome.
-
- 9.6** **CVE-2026-118309** Google Chrome
A remote attacker can execute arbitrary code outside the sandbox via a crafted HTML page in Google Chrome on Android.
-
- 9.6** **CVE-2026-118310** Google Chrome
A remote attacker can execute arbitrary code outside the sandbox via a crafted HTML page in Google Chrome on Windows.
-
- 9.6** **CVE-2026-118312** Google Chrome
A remote attacker can execute arbitrary code outside the sandbox via a crafted HTML page in Google Chrome.
-
- 9.6** **CVE-2026-118321** Google Chrome
A remote attacker can execute arbitrary code outside the sandbox via a crafted HTML page in Google Chrome on Android.
-
- 9.6** **CVE-2026-118340** Google Chrome
A remote attacker can execute arbitrary code outside the sandbox via a crafted HTML page in Google Chrome.
-
- 9.6** **CVE-2026-118316** Google Chrome
A remote attacker can execute arbitrary code outside the sandbox via a crafted HTML page in Google Chrome.
-
- 9.6** **CVE-2026-118332** Google Chrome
A remote attacker can execute arbitrary code outside the sandbox via a crafted HTML page in Google Chrome.
-
- 9.6** **CVE-2026-118342** Google Chrome
A remote attacker can execute arbitrary code outside the sandbox via a crafted HTML page in Google Chrome.
-
- 9.1** **CVE-2026-112352** Sunhillo SureLine
An unauthenticated remote attacker can impersonate any user with an active web session on Sunhillo SureLine.
-

9.9	CVE-2026-104353 Adobe Adobe Campaign Classic	A low-privileged attacker can execute arbitrary code in the context of the current user on Adobe Campaign Classic by injecting malicious OS commands without authentication.
9.8	CVE-2026-35002 pip agno	An attacker can execute arbitrary code on agno via the `field_type` parameter in a `FunctionCall` input field.
9.8	CVE-2026-116692 pip mlflow	An attacker can gain remote code execution on an unauthenticated mlflow server.
9.8	CVE-2026-117532 Redaxo core	An attacker can forge temporary login tokens on REDAXO core, allowing unauthenticated access.

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

Ransomware43

43 victims posted to leak sites. Most active: Booba Project (10), everest (8), play (7), Whitearmor (4), qilin (2).
Financial services hit: Money Concepts Capital (play), NuVista Federal Credit Union (qilin), Hawaii Law Enforcement Fedral Credit Union (qilin).

New data breaches1

AfD	afd.de	345,439 accounts
-----	--------	------------------

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.