

Daily brief, Thursday, October 22, 2026

Oct 21, 8:00 PM to Oct 22, 8:00 PM ET

Generated Oct 29, 2026, 8:49 PM ET

0

Breaking

0

Newly exploited

0

Exploit code

47

Critical CVEs

30

Ransomware posts

0

New breaches

47 new critical CVEs, 30 ransomware posts.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

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

New public exploit code

No new Nuclei templates, Metasploit modules, Exploit-DB or VulnCheck XDB entries.

New critical CVEs

47

- 9.2

CVE-2026-111497 Google Brotli

KEV EXPLOIT CODE

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
- 9.9

CVE-2026-114625 Arista Networks VeloCloud Orchestrator

KEV

A remote attacker can access privileged internal functionality and impact the VeloCloud Orchestrator host without authentication.
- 10.0

CVE-2026-110264 GitLab GitLab

EXPLOIT CODE

An attacker can execute arbitrary code on a GitLab server by exploiting a memory corruption vulnerability.
- 10.0

CVE-2026-110063 Microsoft VM Inspector for Azure Virtual Machines

Improper link resolution before file access ('link following') in VM Inspector for Azure Virtual Machines allows an unauthorized attacker to elevate privileges over a network.

-
- 10.0** **CVE-2026-83938** Microsoft Azure Kubernetes Configuration Service
Missing authentication for critical function in Azure Kubernetes Configuration Service allows an unauthorized attacker to elevate privileges over a network.
-
- 9.1** **CVE-2026-105014** Microsoft Azure Pipelines
An unauthorized attacker can execute code over a network via Azure Pipelines.
-
- 10.0** **CVE-2026-97785** Microsoft Microsoft Entra application proxy
Improper authentication in AAD App Proxy allows an unauthorized attacker to elevate privileges over a network.
-
- 9.5** **ISSUE-GHSA673qmjm6r5xr** npm next
An attacker can execute arbitrary code in Next.js via a crafted `use cache` function.
-
- 9.5** **ISSUE-GHSAcg2gxh64v4q7** npm dompurify
An attacker can bypass sanitization of template expressions in dompurify.
-
- 10.0** **CVE-2026-114575** TOTOLINK A950RG
An attacker can execute arbitrary code on a TOTOLINK A950RG by manipulating the argument of the UploadCustomModule function.
-
- 9.8** **CVE-2021-48014** FanRuan FineReport
An attacker writes arbitrary files on FineReport via a path traversal vulnerability.
-
- 10.0** **CVE-2026-102785** Yootheme.Com YOOtheme Pro extension for Joomla
An attacker can execute arbitrary code on a Joomla site by uploading a malicious image to the YOOtheme Pro extension.
-
- 9.8** **CVE-2022-51026** Bytebase bytebase
An attacker logs in as any user on bytebase without authentication.
-
- 10.0** **CVE-2026-79848** Hewlett Packard Enterprise (HPE) Unknown product
+1 more CVEs in the same release
Vulnerabilities in the affected interface of AOS-8 could allow an unauthenticated remote attacker to conduct SQL injection attacks against an affected AOS-8 instance. Successful exploitation could allow an attacker to execute arbitrary commands on the underlying
-
- 10.0** **CVE-2026-79846** Hewlett Packard Enterprise (HPE) Unknown product
Command injection vulnerabilities exist in the affected interface of AOS-8 that could allow an unauthenticated remote attacker to run arbitrary commands on the underlying host if certain preconditions outside of the attacker's control are met. Successful explo
-
- 10.0** **CVE-2026-79847** Hewlett Packard Enterprise (HPE) Unknown product
Buffer overflow vulnerabilities in the affected interface of AOS-10 could lead to unauthenticated remote code execution by sending specially crafted packets to the affected interface. Successful exploitation of this vulnerability results in the ability to exec
-

10.0**CVE-2026-79851** Hewlett Packard Enterprise (HPE) Unknown product

Buffer overflow vulnerabilities exist in the affected interface of AOS-10 that could lead to unauthenticated remote code execution. Successful exploitation could allow an attacker to execute arbitrary code as a privileged user on the underlying operating system.

9.8**CVE-2021-48016** DedeCMS DedeCMS

An attacker can inject PHP code and execute arbitrary commands on DedeCMS without authentication.

9.5**CVE-2026-97631** TianoCore EDK2

A user with remote access can cause an out-of-bounds write, classic buffer overflow, and incorrect calculation of buffer size in EDK2.

9.8**CVE-2026-79855** Hewlett Packard Enterprise (HPE) ArubaOS (AOS)

An attacker bypasses authentication and gains administrative privileges on ArubaOS.

26 more critical CVEs in this window: see the dashboard

Ransomware

30

30 victims posted to leak sites. Most active: N0n (7), qilin (5), SilentRansomGroup (4), lamashtu (3), akira (3).

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.