Daily brief, Tuesday, November 10, 2026

Nov 9, 7:00 PM to Nov 10, 7:00 PM ET

Generated Nov 10, 2026, 10:08 PM ET

2	0	0	95	88	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

2 breaking, 1 emerging, 95 new critical CVEs, 88 ransomware posts.

Breaking 2

OpenBSD OpenSSH: Auth bypass / access control

- 17 posts from 15 independent sources in 48 h
- OpenSSH: very widely used in large enterprises
- auth bypass / access control
- exploited in the wild (CISA KEV)
- public exploit code
- official advisory

CVEs: CVE-2026-123158

PHP2Shell · PHP

- 12 posts from 8 independent sources in 48 h
- rising: 10 posts in the last 24 h
- PHP: very widely used in large enterprises
- exploited in the wild (CISA KEV)
- public exploit code
- Cloudflare Zero Wire: needs attention

CVEs: CVE-2026-109618, CVE-2026-109619

Emerging 1

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

SonicWall SonicOS

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

CVEs: CVE-2026-19868

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.

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-2024-25420 (7.2), CVE-2026-16065 (6.5)

New critical CVEs 95

10.0 **CVE-2026-120017** SAP SE SAP NetWeaver AS ABAP and ABAP Platform (SAML2 Service Provider)
Unauthenticated attacker bypasses authentication in SAP NetWeaver AS ABAP under certain configurations, impersonating any user including privileged accounts.

10.0 **CVE-2026-76964** SAP SE SAP NetWeaver AS ABAP (Internet Communication Manager)
An unauthenticated attacker sends crafted network traffic to trigger memory corruption in SAP NetWeaver Application Server ABAP; the summary is truncated, so the full impact is not stated.

10.0 **CVE-2026-89103** SAP SE SAP Gateway
Unauthenticated network attacker is treated as an internal application server by SAP Gateway's default ACL, enabling unauthorized actions in SAP Gateway.

10.0 **CVE-2026-89126** SAP SE SAP Web Dispatcher
An unauthenticated attacker can send specially crafted network traffic to SAP Web Dispatcher to trigger a memory corruption condition in an internal component.

9.9 **CVE-2026-109795** SAP SE S4CRM
An attacker with low privileges sends crafted input through a remote interface to execute arbitrary code in SAP NetWeaver, due to missing authorization checks and weak input validation.

9.9 **CVE-2026-109803** SAP SE SAP NetWeaver Knowledge Management (XML Forms)
An authenticated user of SAP NetWeaver Knowledge Management (XML Forms) can get an unauthorized XSL transformation processed, a code injection flaw.

9.9 **CVE-2026-76965** SAP SE SAP NetWeaver and ABAP Platform

Missing authorization checks in SAP NetWeaver AS ABAP and ABAP Platform let a low-privileged attacker run arbitrary OS commands on the host.

9.9 **CVE-2026-120002** Microsoft Microsoft SharePoint Server Subscription Edition

An authorized attacker over the network can elevate privileges in Microsoft Office SharePoint through incorrect authorization checks.

9.8 **CVE-2026-125383** Go2ismail Asp.Net-Core-Inventory-Order-Management-System

INDOTALENT WHMS (Asp.Net-Core-Inventory-Order-Management-System) before 10.20261109 contains an authentication bypass vulnerability caused by a hard-coded JWT signing key, issuer and audience in appsettings.json. Unauthenticated remote attackers can forge toke

9.8 **CVE-2026-121653** Ivanti Endpoint Manager

A remote unauthenticated attacker gets remote code execution via SQL injection in the Core of Ivanti Endpoint Manager before 2024 SU8.

9.8 **CVE-2026-112967** Microsoft Windows 10 Version 1809

Heap-based buffer overflow in Windows Xbox Live Networking Service lets an unauthorized attacker execute code over a network.

9.8 **CVE-2026-114160** Microsoft Azure Managed Grafana

Server-side request forgery in Azure Managed Grafana lets an unauthorized attacker over the network elevate privileges.

9.8 **CVE-2026-116928** Microsoft Windows 10 Version 1607

An unauthorized remote attacker can execute code on systems running the Microsoft Windows Search Component via an out-of-bounds write (CWE-787).

9.8 **CVE-2026-116945** Microsoft Microsoft SQL Server 2017 (GDR)

A heap-based buffer overflow in SQL Server lets an unauthorized remote attacker execute code over the network.

9.8 **CVE-2026-119958** Microsoft Windows 10 Version 1607

An out-of-bounds write in Windows LDAP lets an unauthorized remote attacker execute code over the network.

9.8 **CVE-2026-119990** Microsoft Azure Open AI

Missing authentication for a critical function in Azure OpenAI lets an unauthorized remote attacker elevate privileges over the network.

9.8 **CVE-2026-85844** Microsoft Windows 10 Version 1607

An unauthorized attacker over the network can bypass authentication in Windows Kerberos via an alternate path or channel and elevate privileges.

9.8 **CVE-2026-88218** Microsoft Windows 10 Version 1607

An unauthorized attacker over the network can execute code in Windows DNS via a double free.

9.8 **CVE-2026-88234** Microsoft Windows Server 2016

An unauthorized attacker over the network can execute code in Windows iSCSI via release of an invalid pointer or reference.

9.8 **CVE-2026-88243** Microsoft Windows Server 2016

An unauthorized attacker over the network can execute code in Windows DHCP Server via an out-of-bounds read.

75 more critical CVEs in this window: see the dashboard

Ransomware 88

88 victims posted to leak sites. Most active: inc ransom (45), vortex (9), aoqin leaks (7), obsoft (6), booba team (6).

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.