

Daily brief, Monday, October 26, 2026

Oct 25, 8:00 PM to Oct 26, 8:00 PM ET

Generated Oct 29, 2026, 5:52 PM ET

1

Breaking

2

Newly exploited

2

Exploit code

16

Critical CVEs

33

Ransomware posts

0

New breaches

1 breaking, 3 emerging, 2 newly exploited, 2 with new public exploit code, 16 new critical CVEs, 33 ransomware posts.

Breaking

1

PHP2Shell / Node2Shell · PHP

- 177 posts from 57 independent sources in 48 h
- PHP: very widely used in large enterprises
- remote code execution / auth bypass
- reports of exploitation in the wild
- public exploit code
- named threat actor activity

CVEs: [CVE-2026-111497](#), [CVE-2026-109618](#), [CVE-2026-109619](#), [CVE-2026-115560](#)

Emerging

3

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

Oracle Java SE: Crypto / certificate

- 5 posts from 4 independent sources in 48 h
- Java: very widely used in large enterprises
- remote code execution / auth bypass
- public exploit code
- official advisory

CVEs: [CVE-2026-114820](#)

Arista Networks VeloCloud Orchestrator: SQL injection

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

CVEs: [CVE-2026-114625](#)

Arm Mali Graphics Processing Unit (GPU): Memory corruption

- 6 posts from 4 independent sources in 48 h
- Android: widely used in large enterprises
- exploited in the wild (CISA KEV)

CVEs: [CVE-2022-22706](#)

Newly exploited in the wild

2

9.8

CVE-2026-109618 PHP Group PHP CISA KEV DETECTION

An attacker gains ability to execute arbitrary code by opening a malicious PHP script.

8.1

CVE-2026-109619 PHP Group PHP CISA KEV DETECTION

PHP has a memory corruption vulnerability that can be exploited by an attacker.

New public exploit code

2

9.3

CVE-2026-102782 Ordasoft.Com OrdaSoft Simple Membership extensi... NUCLEI TEMPLATE DETECTION

CVE published Oct 7, 2026

Joomla Extension - ordasoft.com - Unauthenticated SQL injection in OrdaSoft Simple Membership < 7.4.0 - site/simplemembership.php dispatches task=checkLoginPass with no authentication or access control check of any kind. The handler reads a login request param

8.1

CVE-2026-102878 Hangwin mcp-chrome-bridge NUCLEI TEMPLATE DETECTION

CVE published Sep 29, 2026

mcp-chrome-bridge through 1.0.31 contains an origin validation error in the native-server HTTP API that allows attackers to bypass CORS restrictions. Attackers can craft malicious web pages that make cross-origin requests to the local server and invoke browser

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

[CVE-2026-59707 \(8.6\)](#)

New critical CVEs

16

9.8

CVE-2026-116485 Huangxd- danmu api EXPLOIT CODE DETECTION

Affected: danmu_api before 1.21.7. Attacker gains: Ability to modify server environment configuration. Recommended action: Update danmu_api to version 1.21.7 or later.

9.8

CVE-2026-107656 Fortinet FortiSandbox

An attacker can bypass authentication on Fortinet FortiSandbox.

9.9

CVE-2026-116506 TOTOLINK A950RG

An attacker can execute arbitrary code on the TOTOLINK A950RG router by injecting malicious commands remotely.

9.9

CVE-2026-116504 TOTOLINK A950RG

An attacker can execute arbitrary code on the TOTOLINK A950RG router by injecting malicious commands remotely.

9.8

CVE-2026-112346 OpenHands OpenHands Software Agent SDK

An attacker can execute code remotely without authentication on OpenHands Software Agent SDK.

9.8

CVE-2026-107092

An attacker can access files via directory traversal on Nexopos.

9.9

CVE-2026-115188

An attacker can upload arbitrary files to a publicly accessible directory on Mautic 7.

9.1

CVE-2026-116235 Oray Pugongying X5 Pro

A flaw has been found in Oray Pugongying X5 Pro 7.6.1. Affected by this vulnerability is an unknown functionality of the component L2TP Authentication. This manipulation of the argument Username causes crlf injection. The attack may be initiated remotely. The

10.0

CVE-2026-116508 TOTOLINK TOTOLINK

An attacker can cause remote code execution in TOTOLINK A950RG.

9.1

CVE-2026-116234 Oray Pugongying X5 Pro

A vulnerability was detected in Oray Pugongying X5 Pro 7.6.1. Affected is an unknown function of the file /etc/ipsec.conf of the component IPsec Policy Handler. The manipulation of the argument secproto results in crlf injection. The attack can be launched rem

9.1

CVE-2026-116233 Oray Pugongying X5 Pro

A security vulnerability has been detected in Oray Pugongying X5 Pro 7.6.1. This impacts an unknown function of the component Dnsmasq. The manipulation of the argument rent_time leads to crlf injection. The attack can be initiated remotely. The exploit has bee

9.8

CVE-2026-10757 Esri ArcGIS Server

A remote attacker can access the service and potentially execute SQL commands on ArcGIS Server.

9.9

CVE-2026-116231 Oray Pugongying X5 Pro

An attacker can inject malicious code on Oray Pugongying X5 Pro 7.6.1 via a remote attack.

9.9

CVE-2026-116232 Oray Pugongying X5 Pro

An attacker can inject malicious code on Oray Pugongying X5 Pro 7.6.1 via a remote attack.

9.9

CVE-2026-110720 HashiCorp Tooling

An attacker can obtain elevated Consul privileges on the HashiCorp Tooling server without authentication.

9.5

CVE-2026-115905 Zip-Rs zip2

Summary A critical architectural parser differential exists in the `zip` crate (`<= 9.0.4`) between random-access archive readers (`ZipArchive`) and streaming readers (`ZipStreamReader`). `ZipArchive` considers the Central Directory File Header (CDFH) autho

Ransomware

33

33 victims posted to leak sites. Most active: qilin (16), payload (3), Whitearmor (3), emperador (2), rhyssida (1).

Financial services hit: Power Funding (qilin).

New data breaches

No new breaches published.