

Daily brief, Friday, October 23, 2026

Oct 22, 8:00 PM to Oct 23, 8:00 PM ET

Generated Oct 29, 2026, 7:59 PM ET

0

Breaking

2

Newly exploited

0

Exploit code

37

Critical CVEs

40

Ransomware posts

0

New breaches

2 newly exploited, 37 new critical CVEs, 40 ransomware posts.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

2

9.9

CVE-2026-114625 Arista Networks VeloCloud Orchestrator CISA KEV

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

9.8

CVE-2026-110447 Collabora Collabora Online - Built-in CODE Server CISA KEV DETECTION**CVE published Oct 14, 2026**

An attacker can execute remote code.

New public exploit code

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

New critical CVEs

37

9.9

CVE-2026-115893 Bytecodealliance wasmtime EXPLOIT CODE

An attacker can jump to arbitrary code on Wasmtime via a crafted br_table instruction.

9.8

CVE-2026-112398 pip pillow EXPLOIT CODE

Pillow is a Python imaging library. Prior to 13.0.0, Pillow's FlashPix JPEG-tile decoder can write decoded scanlines beyond the allocated tile buffer. FlashPix (FPX) JPEG decoding selects raw mode LA with two bytes per pixel, while an unrecognized JPEG mode ca

9.8

CVE-2026-115812 AWS multi-model-server

Relative path traversal during model archive extraction in Amazon Web Services Multi Model Server 1.1.11 and earlier might allow remote actors to execute arbitrary code via a crafted model archive. Multi Model Server is end of life and no fixed version is avai

9.1

CVE-2026-115547 Okta Okta Access Gateway

An input validation issue in the Okta Access Gateway (OAG) Admin Console allows the processing of specially formatted configuration values. An authenticated administrator can leverage this to execute system commands within the context of the OAG service account

9.9

CVE-2026-77366 npm obsidian-tc

An attacker can access arbitrary configured vaults on obsidian-tc.

9.8

CVE-2026-99079 Linux Linux

The Linux kernel is vulnerable to a denial of service attack.

9.6

CVE-2026-77363 npm obsidian-tc

An attacker can access an Obsidian vault without authentication.

9.5

ISSUE-GHSAcxf39h377rr8 go github.com/labstack/echo/v4

An attacker can bypass Echo route-level access controls via rejected WebSocket upgrades in Echo.

9.8

CVE-2026-53921 Openwrt odhcpd

odhcpd is the DHCPv6, DHCPv4, and router-advertisement server used by OpenWrt. Prior to version 25.12, odhcpd's DHCPv6 IA response handler writes past the end of a fixed 512-byte stack buffer (pdbuf) when a single DHCPv6 REQUEST carries enough IA options to ne

9.9

CVE-2026-115889 rust wasmtime

A large Wasm function body can cause miscompilation in Wasmtime.

9.9

CVE-2026-115931 GitroomHQ postiz-app

An attacker can access internal helper functions on postiz-app, allowing them to read sensitive data.

9.8

CVE-2026-112846 ThemeREX Group Save Life

An attacker can inject objects into the Save Life plugin, allowing arbitrary code execution.

9.8

CVE-2026-112847 ThemeREX ZenSoul

An attacker can inject objects into the ZenSoul plugin, allowing arbitrary code execution.

9.8

CVE-2026-112848 AivahThemes Hostme v2

An attacker can inject objects into the Hostme v2 plugin, allowing arbitrary code execution.

9.8

CVE-2026-112851 ThemeREX Group HotLock

An attacker can inject objects into the HotLock plugin, allowing arbitrary code execution.

9.8

CVE-2026-112853 Axiomthemes Hallelujah

An attacker can inject objects into the Hallelujah plugin, allowing arbitrary code execution.

9.8

CVE-2026-112854 Axiomthemes Holistic Center

An attacker can inject objects into the Holistic Center plugin, allowing arbitrary code execution.

9.8

CVE-2026-112855 Axiomthemes Redy

Deserialization of Untrusted Data vulnerability in axiomthemes Redy redy allows Object Injection. This issue affects Redy: from n/a through 1.3.5.

9.8**CVE-2026-112856** ThemeREX Group Vagabonds

Deserialization of Untrusted Data vulnerability in ThemeREX Group Vagabonds vagabonds allows Object Injection. This issue affects Vagabonds: from n/a through 1.3.10.

9.8**CVE-2026-112857** Axiomthemes Reprizo

Deserialization of Untrusted Data vulnerability in axiomthemes Reprizo reprizo allows Object Injection. This issue affects Reprizo: from n/a through 1.0.8.

17 more critical CVEs in this window: see the dashboard

Ransomware

40

40 victims posted to leak sites. Most active: qilin (10), lockbit5 (4), N0n (4), akira (3), Whitearmor (3).

Financial services hit: SCHWAB-SYSTEM (akira).

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.