# Daily brief, Friday, November 6, 2026

Nov 5, 7:00 PM to Nov 6, 7:00 PM ET

Generated Nov 6, 2026, 11:03 PM ET

| 5 | 0 | 8 | 40 | 23 | 0 |
|---|---|---|---|---|---|
| Breaking | Newly exploited | Exploit code | Critical CVEs | Ransomware posts | New breaches |

5 breaking, 2 emerging, 8 with new public exploit code, 40 new critical CVEs, 23 ransomware posts.

## Breaking 5

### Debian APT

- 15 posts from 13 independent sources in 48 h
- Linux kernel: 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-2026-109518

### Apple safari: Auth bypass / access control

- 14 posts from 13 independent sources in 48 h
- macOS / iOS: very widely used in large enterprises
- auth bypass / access control
- exploited in the wild (CISA KEV)
- named threat actor activity
- official advisory

CVEs: CVE-2024-27834

### Linux

- 13 posts from 10 independent sources in 48 h
- Linux kernel: very widely used in large enterprises
- remote code execution / auth bypass
- public exploit code
- Cloudflare Zero Wire: needs attention

CVEs: CVE-2026-98432

### Zyxel GS1900-24E firmware: Memory corruption (2 CVEs)

- 17 posts from 13 independent sources in 48 h
- remote code execution / auth bypass
- exploited in the wild (CISA KEV)
- public exploit code

CVEs: CVE-2026-107441, CVE-2026-7273

### WordPress Foundation WordPress: Code / command injection

- 10 posts from 10 independent sources in 48 h
- Office: widely used in large enterprises
- code / command injection
- exploited in the wild (CISA KEV)
- public exploit code

CVEs: CVE-2026-119977

## Emerging 2

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

### PHP Group PHP: Memory corruption (2 CVEs)

- 5 posts from 4 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
- Cloudflare Zero Wire: needs attention

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

### SonicWall GMS: Information disclosure

- 3 posts from 3 independent sources in 48 h
- SonicWall: widely used in large enterprises
- remote code execution / auth bypass

CVEs: CVE-2026-109593

## Newly exploited in the wild

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

## New public exploit code 8

9.8 **CVE-2026-120442** Xianhc ape-volo-admin NUCLEI TEMPLATE DETECTION
Unauthenticated attackers forge admin JWTs with a hardcoded signing key in appsettings.json, gaining full admin access to ape-volo-admin before 3.6.1.

7.2 **CVE-2026-116548** E4jvikwp VikRentCar Car Rental Management Syst… NUCLEI TEMPLATE DETECTION
The VikRentCar Car Rental Management System plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'optionals' parameter in all versions up to, and including, 1.4.10 due to insufficient input sanitization and output escaping. This makes it p

5.3 **CVE-2026-119495** WebberZone Better Search NUCLEI TEMPLATE DETECTION
Missing Authorization vulnerability in WebberZone Better Search better-search allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Better Search: from n/a through 4.5.2.

5.3 **CVE-2026-118523** Unknown EventPrime NUCLEI TEMPLATE DETECTION
The EventPrime WordPress plugin before 4.3.6.1 does not keep the built-in Pending Review post status non-public, allowing unauthenticated users to view posts, pages and other content that are awaiting review.

5.3 **CVE-2026-115574** Zulip zulip NUCLEI TEMPLATE DETECTION
Zulip is an open-source team collaboration tool. From 11.0 until 12.2, organizations with web-public channels enabled exposed the GET /json/users endpoint to logged-out spectators, and a missing access-control check allowed include_custom_profile_fields=true t

4.3 **CVE-2026-120597** Welcart e-Commerce Plugin NUCLEI TEMPLATE DETECTION
A vulnerability was identified in Welcart e-Commerce Plugin up to 2.12.6 on WordPress. This affects the function ESCOTT_MAIN::error_page_message of the file classes/paymentESCOTT.main.class.php. Such manipulation of the argument ResponseCd leads to cross site

9.8 **CVE-2026-76519** Cisco Secure Email Gateway METASPLOIT MODULE KEV
**Known since Oct 14, 2026**
Cisco Secure Email Gateway path traversal lets an unauthenticated remote attacker write arbitrary files on the underlying operating system.

9.8 **CVE-2026-76461** Cisco Secure Email Gateway METASPLOIT MODULE KEV
**Known since Sep 14, 2026**
An unauthenticated remote attacker can run arbitrary commands as root on the underlying OS of Cisco Secure Email Gateway (AsyncOS) via SQL injection.

*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-2026-12583 (8.1), CVE-2026-22777 (7.5)

## New critical CVEs 40

10.0 **CVE-2026-109469** Microsoft Entra Device Registration

Authorization bypass via a user-controlled key in Microsoft Entra Device Registration lets an unauthorized attacker over a network elevate privileges.

9.9 **CVE-2026-122193** AWS trusted-remote-execution

Authenticated user with Rex-RO or Rex-RW SSM document access runs arbitrary commands as root via OS command injection in Trusted Remote Execution (REX).

9.9 **ISSUE-GHSAjpf886f3wp38** go github.com/canonical/lxd

A crafted container image lets an attacker read and write arbitrary files on the host running Canonical LXD (github.com/canonical/lxd) through a templates/ symlink.

9.9 **ISSUE-GHSA9j25mm2h2f76** go github.com/canonical/lxd

An attacker gets arbitrary file write on the host through a symlinked exec-output directory in a crafted image in the LXD (github.com/canonical/lxd) container manager.

9.9 **ISSUE-GHSApjffc2wcf6jm** go github.com/canonical/lxd

A malicious image server sending a crafted Incus-Image-Hash header can cause an arbitrary file write in the LXD client, leading to arbitrary command execution as root on the server.

9.9 **ISSUE-GHSAfmc8p6q775cc** go github.com/canonical/lxd

Argument injection via the user-supplied backup compression algorithm in LXD (github.com/canonical/lxd) gives an attacker arbitrary file write on the host and arbitrary code execution.

9.9 **ISSUE-GHSAvghh5rfxxhq8** go github.com/canonical/lxd

A crafted image with a rootfs/ symlink gives an attacker arbitrary file read and write on the host in github.com/canonical/lxd.

9.9 **ISSUE-GHSA47w96r3f938g** go github.com/canonical/lxd

LXD instance snapshots bypass restricted.containers.lowlevel=block, letting an attacker run arbitrary commands on the server via raw.lxc/raw.qemu.

9.8 **CVE-2026-119923** PostgreSQL PostgreSQL

Remote attackers can run arbitrary OS commands as the database process user via a heap overflow in the TDS prelogin parser of Babelfish for PostgreSQL.

9.1 **CVE-2026-114630** Elextensions ELEX WordPress HelpDesk & Customer Ticketing System

Unauthenticated attackers can delete arbitrary files via factory_reset in the ELEX WordPress HelpDesk & Customer Ticketing System plugin through 3.3.8.

9.0 **CVE-2026-63774** Subnet Solutions PowerSYSTEM Center 2024

An authenticated user of PowerSYSTEM Center's report designer can execute unauthorized SQL commands via insufficient input validation (SQL injection).

9.0 **CVE-2026-63017** Subnet Solutions PowerSYSTEM Center 2020

An authenticated low-privileged user of Subnet Solutions PowerSYSTEM Center 2020 can access resources restricted to administrators due to incorrect authorization.

10.0 **CVE-2026-118423** Unknown WP Libre Form
Unauthenticated attackers can upload and execute PHP files via form submissions in WP Libre Form WordPress plugin 1.5.0.1, gaining remote code execution.

10.0 **CVE-2026-71495** Open-Wanderer wanderer
Unauthenticated attacker can make Wanderer before 0.20.0 fetch arbitrary URLs and return the responses (SSRF) when PUBLIC_PRIVATE_INSTANCE is not true.

9.8 **CVE-2026-110955** Unknown Wurdey
Unauthenticated attackers can log in as any administrator with only the username, bypassing signature checks in the Wurdey WordPress plugin through 1.0.0.

9.8 **CVE-2026-113584** Unknown placester
Unauthenticated attackers can overwrite any user's email, including administrators', to take over accounts in the placester WordPress plugin through 1.4.3.

9.8 **CVE-2026-113615** Unknown GS JWT Authentication for WP REST API
Unauthenticated SQL injection in the GS JWT Authentication for WP REST API WordPress plugin through 1.0.0 lets attackers obtain an administrator session.

9.8 **CVE-2026-115230** Unknown WHIZZ
Unauthenticated attackers can set any WordPress user's password, including administrators, taking over accounts in the WHIZZ plugin through 1.1.8.

9.8 **CVE-2026-116533** Unknown Static Snapshot
Unauthenticated attackers can run arbitrary OS commands on the host via Static Snapshot WordPress plugin through 0.2.1 by injecting shell metacharacters.

9.8 **CVE-2026-119516** Mamunur Rashid Radius Booking — Booking Calendar for Appointments & S…
Deserialization of untrusted data in Radius Booking – Booking Calendar for Appointments & Services, versions through 1.0.20, allows object injection by an attacker.

*20 more critical CVEs in this window: see the dashboard*

## Ransomware 23

23 victims posted to leak sites. Most active: n0n (8), leakeddata (3), genesis (2), akira (2), vexy (1).

## 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.