contact@namiq.io · namiq.io

NamiQ

DAILY THREAT WATCH

Daily threat watch

5 November 2026 · 2 exploited CVEs added this week

Analysis Report

2 entries added to CISA's exploited list in the week to 5 November 2026. 1 with a deadline inside three days, in the order to work them.

PREPARED BY	NamiQ	DATE	5 November 2026
FACTS AS OF	5 November 2026	VERSION	1.0
ACT ON NOW	1 of 2	STATUS	Facts as at 5 November 2026

NamiQ © 2026 NamiQ. All rights reserved. This document is the property of NamiQ. It may be shared unaltered, with attribution.
Companion article: namiq.io/insights/daily-threat-watch-2026-11-05

The bottom line

> *Update WordPress core on every site today: CISA lists CVE-2026-119977 as actively exploited with a deadline of 6 November 2026. Apple devices also need updating by 18 November 2026 for CVE-2024-27834.*

CISA added 2 vulnerabilities to its exploited list from 31 October 2026 to 5 November 2026. 1 has a deadline within three days or already past.

Separately, 827 new CVE records were published in the last 30 hours, 129 of them scored 8.5 or higher. They are in the day's CVE highlight, not on this list, because nothing says yet that anyone is using them.

What changed since the last watch

- Left the seven-day window (18): CVE-2026-111357, CVE-2026-118527, CVE-2026-97229, CVE-2026-76418, CVE-2026-46300, CVE-2026-41709, CVE-2026-111497, CVE-2026-48356, CVE-2026-109618, CVE-2026-109619, CVE-2026-104935, CVE-2026-59309, CVE-2026-59310, CVE-2026-47876, CVE-2026-41703, CVE-2024-27833, CVE-2024-27851, CVE-2024-27808.

Since the 4 November 2026 watch: no new entries were added this week. Eighteen items left the week. No deadlines passed between watches.

At a glance

Entry	Act	CISA date	Fixed in	EPSS
WordPress Core (CVE-2026-119977)	Today	Due tomorrow	WordPress 7.1.4	0.01
Apple Multiple Products (CVE-2024-27834)	Next patch cycle	Due in 13 days	Safari 17.5; iOS 17.5 and iPadOS 17.5; iOS 16.7.8 and iPadOS 16.7.8 (older devices); macOS Sonoma 14.5; tvOS 17.5. The record description adds watchOS 10.5. Published 13 May 2024.	0.01

How the week connects

The two items cover unrelated products and different weakness classes. CVE-2024-27834 is an authentication check flaw in Apple WebKit (CWE-287); CVE-2026-119977 is a race condition in WordPress's upgrade path (CWE-367). The record and CISA's text show no connection between them.

Do this today, in this order

- WordPress Core, CVE-2026-119977, due tomorrow. During a WordPress core upgrade, temporary files land at predictable, web-accessible paths. An unauthenticated attacker who times a request there can run code on the server. The record gives CVSS 8.1.

The first hour:

- Go to Dashboard → Updates on each WordPress site and apply the core update now. The CISA deadline is 6 November 2026.
- After updating WordPress, check the access logs and files on each site for unusual requests during any recent upgrade window.
- Check every managed Apple device — Safari, iOS, iPadOS, macOS Sonoma and tvOS — against the fixed versions for CVE-2024-27834; also confirm the watchOS version with the IT provider.
- Ask the IT provider to confirm in writing that both updates are applied and that the WordPress log review found no anomalies.

In the next patch cycle

- Apple Multiple Products, CVE-2024-27834, due in 13 days. The record describes an authentication flaw in Apple WebKit: an attacker with arbitrary read and write access can bypass Pointer Authentication. Affects Safari, iOS, iPadOS, macOS, tvOS and watchOS.

Who can skip most of this

If you run no WordPress sites and no Apple devices or Apple software, neither item this week applies to your systems. That does not mean your systems are free of other flaws on CISA's exploited list.

Send this to your IT provider

Copy it, change the names and dates, and send it. It is a draft for you to check, not a template tested with any provider.

> *Good morning — we need to confirm two CISA items this week. WordPress (CVE-2026-119977): CISA's deadline is 6 November 2026. Please confirm each site is running 7.1.4 or the latest patch for its branch (4.7.39, 4.8.34, 4.9.35, 5.0.31 through 6.9.11, 7.0.8), and that access logs have been checked for unusual requests during any recent core upgrade. Apple (CVE-2024-27834): Please confirm all managed Apple devices are on Safari 17.5, iOS/iPadOS 17.5 (or 16.7.8 on older devices), macOS Sonoma 14.5 or tvOS 17.5. CISA's deadline is 18 November 2026. Please send written confirmation of versions and fix status: WordPress by end of day 6 November 2026, Apple by 17 November 2026. Thank you.*

Check it yourself in two minutes

Everything above comes from public sources. This command prints CISA's additions in the same period with their due dates:

```
curl -s https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json \
  | jq -r '.vulnerabilities[] | select(.dateAdded >= "2026-10-31" and .dateAdded <= "2026-11-
05")
    | [.cveID,.dateAdded,.dueDate,.vendorProject,.product] | @tsv' | sort -k2
```

Run on 5 November 2026 it printed 2 rows, the ones above. A later run may show more.

Check your own project

If you build software, you can compare what a project declares with these CVEs from a terminal. The tool reads requirements files, package.json, Maven, Gradle, Cargo, CMake and Dockerfile files, runs nothing, and only the CVE ids leave your machine. Naming the CVEs needs no key.

```
lattice-scan project . --cve CVE-2026-119977,CVE-2024-27834
```

Each row says in-range, outside-range, undetermined or lead, with the file and line. That is evidence about what a manifest declares, not about what runs, and a person decides. The verdicts, the CSV columns and a pipeline recipe are in the guide.

Check the servers you run

The same ids can be checked against a host. Run this on the machine itself, not on the laptop that deploys to it: it reads installed packages (dpkg, rpm or apk), snaps, the names of running container images and the kernel version, compares them on the spot, and only the CVE ids leave the machine; the inventory stays on it, in ~/.lattice-scan. Naming the CVEs needs no key. Do it on each server after a deployment, and again when a new entry lands.

```
lattice-scan --cve CVE-2026-119977 --cve CVE-2024-27834
```

A match is a candidate for a person to confirm, not a finding. A distribution can fix a CVE under an unchanged version number, so a match is a candidate; on Debian-family hosts the report also shows whether the package's own changelog names the CVE. It reads the names of the running images, not what is inside them; for what an image declares, use the project check on its Dockerfile.

Guide: namiq.io/lattice/guides/choose-your-channel. MCP server (io.namiq/lattice in the MCP registry): namiq.io/lattice. Package: pypi.org/project/lattice-scan, or namiq.io/apt.

What we do not know yet

- Who is using these flaws, and how often. CISA names no attacker and we do not guess one. Ransomware use is as CISA records it; "unknown" means not recorded.
- EPSS is recalculated daily; the figures are as at 5 November 2026 and will have moved. The order is a rule on CISA's dates and EPSS, not a verdict on your estate: check what you run first.
- The bottom line, how the week connects, the first hour, who can skip it and the message are our interpretation of the records, not a statement by CISA or the vendors.

Appendix 1. Timeline

Date	Event
6 November 2026	WordPress Core, CVE-2026-119977: CISA's deadline (added 3 November 2026).
18 November 2026	Apple Multiple Products, CVE-2024-27834: CISA's deadline (added 4 November 2026).

Appendix 2. Definition of done

- Every product on the list was checked against what you run.
- Each one you run has a version, an owner and a date.
- Anything past CISA's deadline is patched or has a written reason and a compensating limit.
- Logs for the weeks before the update were searched for what you patched late.

Sources

- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- CVE record service: https://www.cve.org/