contact@namiq.io · namiq.io

NamiQ

DAILY THREAT WATCH

Daily threat watch

6 November 2026 · 2 exploited CVEs added this week

Analysis Report

2 entries added to CISA's exploited list in the week to 6 November 2026. 1 with a deadline inside three days, in the order to work them.

PREPARED BY	NamiQ	DATE	6 November 2026
FACTS AS OF	6 November 2026	VERSION	1.0
ACT ON NOW	1 of 2	STATUS	Facts as at 6 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-2026-11-06

The bottom line

> *WordPress Core 4.7 through 7.1.3 must be updated to 7.1.4 today — the CISA deadline is 6 November 2026. Apple devices need updates by 18 November 2026 for a separate authentication bypass in iOS, iPadOS, macOS, Safari, tvOS and watchOS.*

CISA added 2 vulnerabilities to its exploited list from 31 October 2026 to 6 November 2026. 1 has a deadline within three days or already past.

Separately, 765 new CVE records were published in the last 30 hours, 89 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 yesterday's watch on 5 November 2026, no new entries were added to the CISA list. Eighteen items left the week. No deadlines passed in that period.

At a glance

Entry	Act	CISA date	Fixed in	EPSS
WordPress Core (CVE-2026-119977)	Today	Due today	WordPress 7.1.4	0.01
Apple Multiple Products (CVE-2024-27834)	Next patch cycle	Due in 12 days	Safari 17.5, iOS 16.7.8 and iPadOS 16.7.8, iOS 17.5 and iPadOS 17.5, macOS Sonoma 14.5, tvOS 17.5, watchOS 10.5	0.01

How the week connects

The two items share no weakness class and come from unrelated product families. CVE-2024-27834 is an authentication mechanism bypass in Apple devices; CVE-2026-119977 is a race condition in WordPress's upgrade process. CISA and the records describe no chain between them.

Do this today, in this order

- WordPress Core, CVE-2026-119977, due today. During a WordPress core upgrade, an unauthenticated attacker can place and run code via predictable, web-accessible staging paths. Any site running WordPress core needs to update to 7.1.4.

The first hour:

- Open Dashboard → Updates on every WordPress site and apply the update to 7.1.4 now; the CISA deadline is today.
- After updating WordPress, check access logs and file integrity on each site for activity during recent upgrade windows.
- Update every Apple device in the firm — iPhone, iPad, Mac, Apple TV and Apple Watch — to the fixed versions for CVE-2024-27834.
- Ask your IT provider for written confirmation that all WordPress sites and Apple devices are on fixed versions.

In the next patch cycle

- Apple Multiple Products, CVE-2024-27834, due in 12 days. The record says an attacker with arbitrary read and write access can bypass Pointer Authentication on Apple devices. Anyone using iOS, iPadOS, macOS, Safari, tvOS or watchOS needs to update.

Who can skip most of this

Firms running no WordPress sites and no Apple devices can skip both items this week. That does not make them safe from other flaws not on this 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.

> *We need your help with two CISA vulnerabilities. CVE-2026-119977 (WordPress Core): the CISA deadline is today, 6 November 2026 — please confirm every WordPress site is on version 7.1.4, and check for any unusual file or access activity from recent upgrade windows. CVE-2024-27834 (Apple devices): deadline 18 November 2026 — please confirm all iPhones, iPads, Macs, Apple TVs and Apple Watches are on Safari 17.5, iOS/iPadOS 17.5 or 16.7.8, macOS Sonoma 14.5, tvOS 17.5 or watchOS 10.5. Please send written confirmation of the installed version and fix status for both items by 7 November 2026.*

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-
06")
    | [.cveID,.dateAdded,.dueDate,.vendorProject,.product] | @tsv' | sort -k2
```

Run on 6 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 6 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/