contact@namiq.io · namiq.io

NamiQ

DAILY THREAT WATCH

Daily threat watch

8 November 2026 · 3 exploited CVEs added this week

Analysis Report

3 entries added to CISA's exploited list in the week to 8 November 2026. 1 with a deadline inside three days, in the order to work them.

PREPARED BY	NamiQ	DATE	8 November 2026
FACTS AS OF	8 November 2026	VERSION	1.0
ACT ON NOW	1 of 3	STATUS	Facts as at 8 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-2026-11-08

The bottom line

> *The WordPress CISA deadline of 6 November 2026 has passed; any site still below 7.1.4 is overdue and must be updated now. The Apple and SonicWall SonicOS SSLVPN deadlines fall on 18 and 20 November 2026 respectively; check those installations this week.*

CISA added 3 vulnerabilities to its exploited list from 3 November 2026 to 8 November 2026. 1 has a deadline within three days or already past, 1 of them past.

Separately, 339 new CVE records were published in the last 30 hours, 84 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.

No new items were added since the 7 November 2026 watch. Eighteen items left the week, including CVE-2024-27833, CVE-2024-27851 and CVE-2024-27808. No deadlines passed since the last watch.

At a glance

Entry	Act	CISA date	Fixed in	EPSS
WordPress Core (CVE-2026-119977)	Today	2 days past CISA's deadline	WordPress 7.1.4	0.01
Apple Multiple Products (CVE-2024-27834)	Next patch cycle	Due in 10 days	Safari 17.5; iOS 16.7.8 and 17.5; iPadOS 16.7.8 and 17.5; macOS Sonoma 14.5; tvOS 17.5; watchOS 10.5 (per the CVE record, published 13 May 2024).	0.02
SonicWall SonicOS SSLVPN (CVE-2026-19868)	Next patch cycle	Due in 12 days	The record does not name a fixed version; the unaffected list is empty. No vendor advisory could be read. Contact SonicWall for the first version that removes this flaw.	0.01

How the week connects

Two of the three items share an authentication weakness class: CVE-2024-27834 (Apple, CWE-287 Improper Authentication) and CVE-2026-19868 (SonicWall, CWE-308 Use of Single-factor Authentication) both weaken how identity is verified. CVE-2026-119977 (WordPress, CWE-367) is a timing flaw during upgrades and shares no weakness class with the other two; the records do not describe chaining between any of the three.

Do this today, in this order

- WordPress Core, CVE-2026-119977, 2 days past CISA's deadline. WordPress core uses predictable, web-accessible staging paths during full-package upgrades that an unauthenticated attacker can reach to run code on the server. CISA's 6 November 2026 deadline has passed; update to 7.1.4 now.

The first hour:

- Check every WordPress site and update to 7.1.4 or the latest patch for your branch; the CISA deadline of 6 November 2026 has already passed.
- Update all Apple devices — iPhone, iPad, Mac, Apple TV and Apple Watch — to the fixed releases; deadline is 18 November 2026.
- Contact SonicWall to confirm which SonicOS release addresses CVE-2026-19868; no fixed version is stated in the CVE record; deadline is 20 November 2026.

In the next patch cycle

- Apple Multiple Products, CVE-2024-27834, due in 10 days. An attacker with arbitrary read and write access on an Apple device can bypass Pointer Authentication, a hardware barrier against reliable code execution. The record lists iPhone, iPad, Mac, Apple TV and Apple Watch.
- SonicWall SonicOS SSLVPN, CVE-2026-19868, due in 12 days. The record says a user with credentials for any alternate authentication method can bypass SAML controls and any MFA SAML enforces on SonicWall SonicOS SSLVPN. Anyone running this VPN with SAML authentication must act before 20 November 2026.

Who can skip most of this

Organisations running no WordPress sites, no Apple devices (iPhone, iPad, Mac, Apple TV or Apple Watch) and no SonicWall SonicOS SSLVPN can skip most of this week. This does not mean they are unaffected by other flaws in CISA's catalogue.

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 are writing about three CISA-listed vulnerabilities affecting products we may run. Could you please confirm the status of each by 14 November 2026? 1. WordPress (CVE-2026-119977): the CISA deadline was 6 November 2026. Please confirm every WordPress site is on 7.1.4 or the latest patch for its branch. 2. Apple devices — iPhone, iPad, Mac, Apple TV, Apple Watch (CVE-2024-27834): deadline 18 November 2026. Please confirm all devices are on the fixed releases. 3. SonicWall SonicOS SSLVPN (CVE-2026-19868): deadline 20 November 2026. No fixed version is stated in the CVE record; please contact SonicWall and confirm which release addresses this flaw. Please reply with the confirmed version and fix status for each. 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 >= "2026-11-03" and .dateAdded <= "2026-11-
08")
    | [.cveID,.dateAdded,.dueDate,.vendorProject,.product] | @tsv' | sort -k2
```

Run on 8 November 2026 it printed 3 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,CVE-2026-19868
```

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 hardware (maker, model, firmware), the running container images with their operating system and packages, 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 --cve CVE-2026-19868
```

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. By default it opens the images your containers are running and reads their operating system and package list; a deep scan (--deep, a few minutes) opens every local image and the Python, Node, Java and Ruby packages 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 8 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).
20 November 2026	SonicWall SonicOS SSLVPN, CVE-2026-19868: CISA's deadline (added 6 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/