contact@namiq.io · namiq.io

NamiQ

DAILY THREAT WATCH

Daily threat watch

9 November 2026 · 3 exploited CVEs added this week

Analysis Report

3 entries added to CISA's exploited list in the week to 9 November 2026. 1 with a deadline inside three days, in the order to work them.

PREPARED BY	NamiQ	DATE	9 November 2026
FACTS AS OF	9 November 2026	VERSION	1.0
ACT ON NOW	1 of 3	STATUS	Facts as at 9 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-2026-11-09

The bottom line

> *The CISA deadline for CVE-2026-119977 (WordPress Core) passed on 6 November; update every WordPress site now and check access logs and files for signs of prior compromise. CVE-2024-27834 (Apple devices) and CVE-2026-19868 (SonicWall SSLVPN) have deadlines on 18 and 20 November respectively.*

CISA added 3 vulnerabilities to its exploited list from 3 November 2026 to 9 November 2026. 1 has a deadline within three days or already past, 1 of them past.

Separately, 356 new CVE records were published in the last 30 hours, 62 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 watch of 8 November 2026, no new CVEs were added to the week. Eighteen entries left the week. No deadlines passed in the interval since the previous watch; the WordPress deadline had already passed before that watch.

At a glance

Entry	Act	CISA date	Fixed in	EPSS
WordPress Core (CVE-2026-119977)	Today	3 days past CISA's deadline	WordPress 7.1.4	0.01
Apple Multiple Products (CVE-2024-27834)	Next patch cycle	Due in 9 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 11 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

The Apple (CWE-287) and SonicWall (CWE-308) items both weaken authentication controls, though on unrelated products with different mechanisms; the record does not say they can be chained. The WordPress item (CWE-367) is a timing flaw in the upgrade process and belongs to a different weakness class; it has no stated link to the other two.

Do this today, in this order

- WordPress Core, CVE-2026-119977, 3 days past CISA's deadline. WordPress Core 4.7 through 7.1.3 — an unauthenticated attacker can run code on the server during a core upgrade. CISA's deadline passed 6 November; update now and check for prior compromise.

The first hour:

- Open the WordPress dashboard on every managed site. If the version is below 7.1.4 or the latest patch of your branch, apply the update immediately.
- On all managed Apple devices, confirm the OS and Safari versions meet the fixed releases for CVE-2024-27834; prioritise devices used for web browsing.
- Contact SonicWall support to identify the first release that addresses CVE-2026-19868; the record names no fixed version.
- On any WordPress site that ran a core upgrade before today, check server access logs and site files for signs of unauthorised access.

In the next patch cycle

- Apple Multiple Products, CVE-2024-27834, due in 9 days. Apple iOS, iPadOS, macOS, Safari, tvOS and watchOS — an attacker with arbitrary read and write access on the device can bypass Pointer Authentication. The record names fixes for all six platforms.
- SonicWall SonicOS SSLVPN, CVE-2026-19868, due in 11 days. SonicWall SonicOS SSLVPN — a user with valid alternate-method credentials can bypass SAML authentication controls and any MFA that SAML enforces. Relevant to anyone running a SonicWall VPN with SAML.

Who can skip most of this

Organisations running no WordPress sites, no Apple devices or browsers, and no SonicWall VPN can pass over most of this week's items. That does not indicate they are free of other exploited flaws.

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 written confirmation of the status of three CISA-listed vulnerabilities. CVE-2026-119977 (WordPress Core) — CISA's deadline passed on 6 November. Please confirm every WordPress site is on 7.1.4 or the latest patch of its branch, and that you have checked access logs for signs of compromise. CVE-2024-27834 (Apple iOS, iPadOS, macOS, Safari, tvOS, watchOS) — deadline 18 November 2026. Please confirm all affected devices are on their fixed versions. CVE-2026-19868 (SonicWall SonicOS SSLVPN) — deadline 20 November 2026. The record names no fixed version; please contact SonicWall to identify which release addresses this flaw. We would like written confirmation of version and fix status for each by 13 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 >= "2026-11-03" and .dateAdded <= "2026-11-09")
    | [.cveID,.dateAdded,.dueDate,.vendorProject,.product] | @tsv' | sort -k2
```

Run on 9 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 9 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/