contact@namiq.io · namiq.io

NamiQ

DAILY THREAT WATCH

Daily threat watch

7 November 2026 · 3 exploited CVEs added this week

Analysis Report

3 entries added to CISA's exploited list in the week to 7 November 2026. 1 with a deadline inside three days, in the order to work them.

PREPARED BY	NamiQ	DATE	7 November 2026
FACTS AS OF	7 November 2026	VERSION	1.0
ACT ON NOW	1 of 3	STATUS	Facts as at 7 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-2026-11-07

The bottom line

> *The WordPress deadline (CVE-2026-119977) passed on 6 November 2026; confirm that every WordPress site is at 7.1.4 or its backport now, then check access logs and files for signs of access during recent upgrades. The SonicWall and Apple deadlines fall on 20 and 18 November respectively.*

CISA added 3 vulnerabilities to its exploited list from 1 November 2026 to 7 November 2026. 1 has a deadline within three days or already past, 1 of them past.

Separately, 844 new CVE records were published in the last 30 hours, 164 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

- Deadline passed since: WordPress Core, CVE-2026-119977.
- 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 6 November 2026 watch, no new entries were added. Eighteen items left the week. The CISA deadline for CVE-2026-119977 (WordPress Core) passed on 6 November 2026.

At a glance

Entry	Act	CISA date	Fixed in	EPSS
WordPress Core (CVE-2026-119977)	Today	1 day past CISA's deadline	WordPress 7.1.4	0.01
Apple Multiple Products (CVE-2024-27834)	Next patch cycle	Due in 11 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 13 days	Not stated; see the note	n/a

How the week connects

CVE-2026-19868 (CWE-308) and CVE-2024-27834 (CWE-287) both involve authentication controls being bypassed, but affect different products and the records show no link between them. CVE-2026-119977 (CWE-367) is a race condition during software upgrades and has no connection to either.

Do this today, in this order

- WordPress Core, CVE-2026-119977, 1 day past CISA's deadline. WordPress Core. During a core upgrade, predictable web-reachable staging paths allow an unauthenticated attacker to run code on the server. Anyone who operates a WordPress site must act.

The first hour:

- Confirm that every WordPress site is on 7.1.4 or the matching backport for its branch — the CISA deadline passed on 6 November 2026.
- On each updated WordPress site, check access logs and file timestamps for unusual activity during any recent upgrade window.
- Confirm all Apple devices (iPhones, iPads, Macs, Apple TVs, Apple Watches) are on the fixed releases for CVE-2024-27834.
- If you run SonicWall SonicOS SSLVPN with SAML enabled, check the firmware version and whether the vendor has published a fix for CVE-2026-19868.

In the next patch cycle

- Apple Multiple Products, CVE-2024-27834, due in 11 days. Affects iPhones, iPads, Macs, Apple TVs and Apple Watches. An attacker with arbitrary read and write access can bypass Pointer Authentication, a hardware barrier against memory-corruption exploits.
- SonicWall SonicOS SSLVPN, CVE-2026-19868, due in 13 days. Affects SonicWall SonicOS SSLVPN with SAML configured. The record says a user with valid credentials for any alternate login method can bypass SAML controls, including SAML-enforced MFA.

Who can skip most of this

Organisations running none of SonicWall SonicOS SSLVPN, Apple devices (iPhone, iPad, Mac, Apple TV, Apple Watch), or WordPress can set this week aside, though that does not address other flaws in their estate.

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 are writing about three CISA Known Exploited Vulnerabilities. The deadline for CVE-2026-119977 (WordPress Core) passed on 6 November 2026 — please confirm in writing which version each of our WordPress sites is running and that it is at 7.1.4 or the matching backport. The Apple devices deadline (CVE-2024-27834: iOS, iPadOS, macOS, Safari, tvOS, watchOS) falls on 18 November — please confirm all devices are on the fixed releases. The SonicWall SSLVPN deadline (CVE-2026-19868) falls on 20 November — please confirm the firmware version, whether SAML is configured, and whether a vendor fix is available. Please respond in writing by 14 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 >= "2026-11-01" and .dateAdded <= "2026-11-
07")
    | [.cveID,.dateAdded,.dueDate,.vendorProject,.product] | @tsv' | sort -k2
```

Run on 7 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 7 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/