contact@namiq.io · namiq.io

NamiQ

DAILY THREAT WATCH

Daily threat watch

6 November 2026 · 3 exploited CVEs added this week

Analysis Report

3 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 3	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 (CVE-2026-119977) has a CISA deadline of 6 November 2026 — today; update every WordPress site to 7.1.4 or the matching branch patch immediately. SonicWall SSLVPN (CVE-2026-19868) and Apple devices (CVE-2024-27834) have deadlines of 20 and 18 November 2026 respectively.*

CISA added 3 vulnerabilities to its exploited list from 1 November 2026 to 6 November 2026. 1 has a deadline within three days or already past.

Separately, 626 new CVE records were published in the last 30 hours, 99 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

- New: SonicWall SonicOS SSLVPN, CVE-2026-19868.
- 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, CVE-2026-19868 (SonicWall SonicOS SSLVPN) is new. Eighteen entries left the week's list. No deadlines passed since yesterday.

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	0.02
SonicWall SonicOS SSLVPN (CVE-2026-19868)	Next patch cycle	Due in 14 days	Not stated in the sources reviewed.	n/a

How the week connects

CVE-2026-19868 and CVE-2024-27834 both describe authentication weaknesses — one allowing bypass of SAML controls on a VPN service, one allowing bypass of a device-level protection — though they affect unrelated products and no source shows them linked. CVE-2026-119977 is a race condition during a web platform upgrade; it shares neither the weakness type nor the product class with the other two.

Do this today, in this order

- WordPress Core, CVE-2026-119977, due today. During a WordPress core upgrade, predictable web-accessible staging paths let an unauthenticated attacker run code on the server. Update to 7.1.4 or the matching branch patch immediately.

The first hour:

- Check every WordPress site: open Dashboard → Updates and apply the update if the version is below 7.1.4 or the matching branch patch. CISA's deadline is today, 6 November 2026.
- On every Apple device — iPhone, iPad, Mac, Apple TV, Apple Watch — check the software version and apply any available update before 18 November 2026.
- If you run SonicWall SonicOS SSLVPN, confirm the firmware version and whether SAML is enabled, then ask SonicWall for a patched release before 20 November 2026.
- For WordPress, after updating, check access logs and site files for unexpected access during any recent core upgrade window.

In the next patch cycle

- Apple Multiple Products, CVE-2024-27834, due in 12 days. An attacker who already has arbitrary read and write access on an Apple device can bypass Pointer Authentication. Affects iPhone, iPad, Mac, Apple TV, and Apple Watch.
- SonicWall SonicOS SSLVPN, CVE-2026-19868, due in 14 days. An attacker holding any non-SAML credentials can bypass SAML authentication controls on SonicWall SSLVPN, defeating SAML-enforced MFA. Organisations running this service with SAML enabled must act.

Who can skip most of this

Organisations that run no WordPress sites, no SonicWall SSLVPN gateways, and no Apple devices can skip most of the steps above. This does not mean they are unaffected by other flaws active this week.

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. Please confirm three CISA-listed vulnerabilities in writing. 1. CVE-2026-119977 — WordPress Core: version on each site and whether updated to 7.1.4 (or matching branch patch). CISA's deadline is 6 November 2026 — please confirm by today. 2. CVE-2024-27834 — Apple iOS, iPadOS, macOS, Safari, tvOS, watchOS: software version on each device and whether updated. Please confirm before 18 November 2026. 3. CVE-2026-19868 — SonicWall SonicOS SSLVPN: firmware version, whether SAML is enabled, and what SonicWall recommends (no fixed version is stated in the record). Please confirm before 20 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 >= "2026-11-01" and .dateAdded <= "2026-11-
06")
    | [.cveID,.dateAdded,.dueDate,.vendorProject,.product] | @tsv' | sort -k2
```

Run on 6 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 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).
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/