contact@namiq.io · namiq.io

NamiQ

DAILY THREAT WATCH

Daily threat watch

4 November 2026 · 4 exploited CVEs added this week

Analysis Report

4 entries added to CISA's exploited list in the week to 4 November 2026. 2 with a deadline inside three days, in the order to work them.

PREPARED BY	NamiQ	DATE	4 November 2026
FACTS AS OF	4 November 2026	VERSION	1.0
ACT ON NOW	2 of 4	STATUS	Facts as at 4 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-2026-11-04

The bottom line

> *If you run WordPress, update every site to version 7.1.4 today — CISA's deadline is 6 November 2026. If you run Ivanti Connect Secure, the deadline for CVE-2026-111357 passed on 2 November 2026 and the patch must be applied without delay.*

CISA added 4 vulnerabilities to its exploited list from 30 October 2026 to 4 November 2026. 2 have a deadline within three days or already past, 1 of them past.

Separately, 824 new CVE records were published in the last 30 hours, 135 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: Apple Multiple Products, CVE-2024-27834.
- Left the seven-day window: 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-2026-104935, CVE-2026-104935, CVE-2026-104935, CVE-2026-109618, CVE-2026-109619, CVE-2026-109618, CVE-2026-109619, CVE-2026-59309, CVE-2026-59310, CVE-2026-47876, CVE-2026-59309, CVE-2026-59310, CVE-2026-47876, CVE-2026-41703, CVE-2026-109619, CVE-2026-109618, CVE-2026-104935, CVE-2026-104935, CVE-2026-104935, CVE-2026-104935, CVE-2026-109618, CVE-2026-109619, CVE-2026-109618, CVE-2026-109619, CVE-2026-59309, CVE-2026-59310, CVE-2026-47876, CVE-2026-59309, CVE-2026-59310, CVE-2026-47876, CVE-2026-41703, CVE-2026-48356, CVE-2026-48356, CVE-2026-111497, CVE-2026-111497, CVE-2026-104935, CVE-2026-104935, CVE-2026-104935, CVE-2026-104935, CVE-2026-46300, CVE-2026-109618, CVE-2026-109619, CVE-2026-46300, CVE-2026-109618, CVE-2026-109619, CVE-2026-41709, CVE-2026-41709, CVE-2026-59309, CVE-2026-59310, CVE-2026-47876, CVE-2026-59309, CVE-2026-59310, CVE-2026-47876, CVE-2026-41703, CVE-2026-41709, CVE-2026-104935, CVE-2026-104935, CVE-2026-104935, CVE-2026-104935, CVE-2026-104935, CVE-2026-97229, CVE-2026-76418.

Since 3 November 2026, one entry was added: CVE-2024-27834 covering Apple iOS, iPadOS, macOS, Safari, tvOS and watchOS. Many items left the week's list. No deadlines passed since the previous watch.

At a glance

Entry	Act	CISA date	Fixed in	EPSS

Ivanti Connect Secure (CVE-2026-111357)	Today	2 days past CISA's deadline	Not stated; see the note	0.01
WordPress Core (CVE-2026-119977)	Today	Due in 2 days	WordPress 7.1.4	0.01
Ivanti Connect Secure (CVE-2026-118527)	Next patch cycle	Due in 9 days	Ivanti Connect Secure 25.1.1.3 and 22.8R2.6, as the record states.	0.01
Apple Multiple Products (CVE-2024-27834)	Next patch cycle	Due in 14 days	Safari 17.5; iOS 17.5 and iPadOS 17.5; iOS 16.7.8 and iPadOS 16.7.8; macOS Sonoma 14.5; tvOS 17.5; watchOS 10.5 (record, 13 May 2024).	0.01

How the week connects

The two Ivanti Connect Secure entries chain with each other and with CVE-2026-104935, which left this week's list; both records say the three can be combined. The Apple flaw requires arbitrary read and write access first, making it a step in a chain rather than a standalone attack. The WordPress flaw shares no weakness class or product family with the others.

Do this today, in this order

- Ivanti Connect Secure, CVE-2026-111357, 2 days past CISA's deadline. An attacker on Ivanti Connect Secure can escalate to root through a function that lacks proper authentication. The record says this flaw chains with CVE-2026-104935 and CVE-2026-118527.
- WordPress Core, CVE-2026-119977, due in 2 days. During a WordPress core upgrade, an unauthenticated attacker can time a request to place or run code on the server. Any publicly reachable WordPress installation must be updated to 7.1.4.

The first hour:

- Check whether any WordPress sites are running a version below 7.1.4; if so, go to Dashboard → Updates on each site and apply the core update now.
- Check whether Ivanti Connect Secure is in use; if so, confirm it is patched — CISA's deadline for CVE-2026-111357 passed on 2 November 2026.
- On all Apple devices, confirm iOS, iPadOS, macOS, Safari, tvOS and watchOS are on the versions listed for CVE-2024-27834; deadline is 18 November 2026.
- For Ivanti Connect Secure, confirm the version is 25.1.1.3 or 22.8R2.6 to cover CVE-2026-118527; deadline is 13 November 2026.

In the next patch cycle

- Ivanti Connect Secure, CVE-2026-118527, due in 9 days. An authenticated attacker on Ivanti Connect Secure can upload files with controlled content to a known location on disk. The record says this flaw chains with CVE-2026-111357.
- Apple Multiple Products, CVE-2024-27834, due in 14 days. An attacker who already has arbitrary read and write access on an Apple device can bypass pointer authentication. Anyone running Apple iOS, iPadOS, macOS, Safari, tvOS or watchOS should update.

Who can skip most of this

Organisations running no WordPress sites, no Ivanti Connect Secure appliances, and no Apple devices can skip most of this week's items. That does not mean they face no threats from other sources.

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 written confirmation on four items from CISA's known-exploited list. WordPress (CVE-2026-119977): confirm every site runs version 7.1.4 or later. CISA's deadline is 6 November 2026. Ivanti Connect Secure (CVE-2026-111357): CISA's deadline passed on 2 November 2026. Confirm the patch is applied and state the installed version. Ivanti Connect Secure (CVE-2026-118527): confirm the version is 25.1.1.3 or 22.8R2.6. Deadline is 13 November 2026. Apple devices (CVE-2024-27834): confirm all iOS, iPadOS, macOS, Safari, tvOS and watchOS are updated to the fixed versions. Deadline is 18 November 2026. Please reply with installed versions and confirmation of each fix by 5 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 >= "2026-10-30" and .dateAdded <= "2026-11-
04")
    | [.cveID,.dateAdded,.dueDate,.vendorProject,.product] | @tsv' | sort -k2
```

Run on 4 November 2026 it printed 4 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-2026-111357,CVE-2026-119977,CVE-2026-118527,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-2026-111357 --cve CVE-2026-119977 --cve CVE-2026-118527 --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 4 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
2 November 2026	Ivanti Connect Secure, CVE-2026-111357: CISA's deadline (added 30 October 2026).
6 November 2026	WordPress Core, CVE-2026-119977: CISA's deadline (added 3 November 2026).
13 November 2026	Ivanti Connect Secure, CVE-2026-118527: CISA's deadline (added 30 October 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/