contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Apple Multiple Products exploited

CVE-2024-27834 · on CISA's exploited list since 4 November 2026

Analysis Report

Anyone running unpatched Apple devices should update by 18 November 2026 — CISA's deadline. Update iOS, iPadOS, macOS, Safari, tvOS and watchOS to the fixed versions; if no Apple devices are in use …

PREPARED BY	NamiQ	DATE	4 November 2026
FACTS AS OF	4 November 2026	VERSION	1.0
SEVERITY	**High: CVSS 3.1 8.1**	STATUS	On CISA's exploited list; due 18 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/apple-multiple-products-cve-2024-27834

The bottom line

> *Anyone running unpatched Apple devices should update by 18 November 2026 — CISA's deadline. Update iOS, iPadOS, macOS, Safari, tvOS and watchOS to the fixed versions; if no Apple devices are in use, nothing to do here.*

At a glance

Fact	Detail
Product	Apple Multiple Products (CVE-2024-27834)
Severity	High: 8.1 (CVSS 3.1)
CISA	On its exploited list since 4 November 2026. Deadline for US federal agencies: 18 November 2026.
Chance of exploitation (EPSS)	0.01, the estimated chance in the next 30 days, as at 4 November 2026
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	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).
Who looks first	Anyone who manages or uses iPhone, iPad, Mac, Apple TV or Apple Watch. The flaw is in WebKit, which underpins Safari and every browser engine on iOS and iPadOS, so all users of those platforms are in scope.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you manage or use any Apple device — iPhone, iPad, Mac, Apple TV or Apple Watch?	Nothing to do for this CVE.	Check the software version on each device.
Is any iOS or iPadOS device below version 17.5 (or below 16.7.8 on eligible older hardware)?	Check macOS, tvOS and watchOS versions below.	Update to iOS 17.5 or iPadOS 17.5 (or 16.7.8 for older eligible devices).
Is any Mac running macOS below Sonoma 14.5, or is Safari below version 17.5?	Check tvOS and watchOS.	Update macOS to Sonoma 14.5, or update Safari to 17.5.

Is any Apple TV running tvOS below 17.5, or any Apple Watch running watchOS below 10.5?	Nothing further for this CVE.	Update to tvOS 17.5 or watchOS 10.5.

What it is

The record says an attacker who already has arbitrary read and write access on the device may be able to bypass Pointer Authentication — a hardware-enforced defence that prevents memory corruption from being escalated into full code execution.

Why it matters

Our reading is that this flaw is a step in an exploit chain rather than a standalone attack: an attacker needs arbitrary read and write access first, which other WebKit flaws fixed in the same release — CVE-2024-27833, CVE-2024-27851 and CVE-2024-27808 — could supply by processing maliciously crafted web content. CISA rates this at 8.1, higher than the record's 5.5, which reflects how the flaws combine. Patching removes the whole chain at once.

What the vendor's advisory says

We read three pages on support.apple.com. In short:

- The vendor's advisory (Safari 17.5, 13 May 2024) also patches CVE-2024-27833 (WebKit): processing maliciously crafted web content may lead to arbitrary code execution via an integer overflow.
- CVE-2024-27851 in the same release (WebKit): processing maliciously crafted web content may lead to arbitrary code execution via a bounds-check failure.
- CVE-2024-27808 in the same release (WebKit): processing web content may lead to arbitrary code execution.
- CVE-2024-27820 in the same release (WebKit Web Inspector): processing web content may lead to arbitrary code execution.
- CVE-2024-27856, added to the advisory 15 January 2025 (WebKit): processing a file may lead to unexpected app termination or arbitrary code execution.

Things people will get wrong

- This flaw alone lets an attacker take over a device from the internet. The record says the attacker must already have arbitrary read and write capability on the device. This flaw extends what they can then do; it is not an entry point on its own.
- Only Safari on Mac is affected. The record lists iOS, iPadOS, macOS, tvOS and watchOS as affected. On iOS and iPadOS, all browser engines use WebKit, so the exposure is not limited to the Safari app.

How we would triage it

This is our judgement.

Step 1: Find the software versions you run

- On iPhone and iPad, go to Settings → General → About and note the iOS or iPadOS version. The record gives fixed versions as 17.5 or 16.7.8.
- On Mac, check the macOS and Safari versions. The record says macOS Sonoma 14.5 and Safari 17.5 are fixed.

Step 2: Apply all available Apple software updates

- On iPhone and iPad, go to Settings → General → Software Update and install any available update. The record says iOS 17.5 and iPadOS 17.5 (or 16.7.8 for older eligible devices) contain the fix.
- On Mac, open System Settings → General → Software Update. The record says macOS Sonoma 14.5 contains the fix.

Step 3: Verify managed devices are updated

- If devices are managed via MDM, confirm the update policy has delivered iOS 17.5 or iPadOS 17.5 (or 16.7.8) to all enrolled devices.
- Check Apple TV and Apple Watch: the record names tvOS 17.5 and watchOS 10.5 as fixed versions.

Step 4: Review devices that browsed untrusted content before patching

- Check Safari crash logs on any device that was unpatched and used for web browsing. The flaw is in WebKit, so unexpected crashes during browsing are the indicator to look for.

To close it, read the version from the product itself, not from an old inventory, and save the output with the date. If you cannot update today, write down who owns it, the new date, and what limits exposure until then. CISA's wording adds that you should stop using the product if no mitigation is available.

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 regarding CVE-2024-27834, a WebKit vulnerability affecting Apple iOS, iPadOS, macOS, Safari, tvOS and watchOS. CISA has listed it with a remediation deadline of 18 November 2026. The fix is in iOS 17.5 and iPadOS 17.5 (or 16.7.8 for older eligible devices), macOS Sonoma 14.5, Safari 17.5, tvOS 17.5 and watchOS 10.5. Could you please confirm: (1) which Apple devices and software versions we are currently running, (2) whether any are below the fixed versions, and (3) if so, what the update plan is and when it will complete. We would like written confirmation of the current versions and the fix applied by 14 November 2026.*

Signs it was used

An update closes the hole. It does not tell you whether someone used it first. CISA's required action points to its forensic triage requirements (BOD 26-04). Look for:

- Unexpected crashes or terminations in Safari or other WebKit-based apps during or after browsing sessions on devices that were unpatched.
- Crash reports in /Library/Logs/DiagnosticReports or ~/Library/Logs/DiagnosticReports on Mac, naming WebKit or Safari processes, with timestamps matching the period when the device was unpatched.
- Unusual process activity following web browsing — unexpected child processes spawned by WebKit or Safari beyond what normal browsing produces.

The weakness behind it

CISA's entry classes this as CWE-287 (Improper Authentication).

The sources, in their words

CISA's catalogue entry:

> *Apple iOS, iPadOS, macOS, Safari, tvOS and watchOS 10.5 contain an improper authentication vulnerability which could allow an attacker with arbitrary read and write capability to bypass pointer authentication.*

The CVE record, published by Apple on 13 May 2024:

> *The issue was addressed with improved checks. This issue is fixed in 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. An attacker with arbitrary read and write capability may be able to bypass Pointer Authentication.*

Versions of Apple Safari the record lists as affected:

- all versions before 17.5

The affected ranges end before 17.5. Those are the first versions the record does not list as affected; confirm them in the vendor's advisory.

Versions of Apple iOS and iPadOS the record lists as affected:

- all versions before 16.7.8
- all versions before 17.5

The affected ranges end before 16.7.8, 17.5. Those are the first versions the record does not list as affected; confirm them in the vendor's advisory.

Versions of Apple macOS the record lists as affected:

- all versions before 14.5

The affected ranges end before 14.5. Those are the first versions the record does not list as affected; confirm them in the vendor's advisory.

Versions of Apple tvOS the record lists as affected:

- all versions before 17.5

The affected ranges end before 17.5. Those are the first versions the record does not list as affected; confirm them in the vendor's advisory.

CISA's required action:

> *Apply mitigations in accordance with vendor instructions.*

Check your own project

If you build software, you can compare what a project declares with this CVE from a terminal. The tool reads requirements files, package.json, Maven, Gradle, Cargo, CMake and Dockerfile files, runs nothing, and only the CVE id leaves your machine. Naming the CVEs needs no key.

```
lattice-scan project . --cve 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 id 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-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

- The sources do not say whether this flaw has been paired with another exploit in an observed attack, or which specific CVE would supply the required arbitrary read and write access in a real chain.
- The sources do not explain why CISA added this flaw in November 2026, more than two years after Apple released the patch on 13 May 2024.
- The sources do not say which Apple chip generations are required for the Pointer Authentication feature — older devices without it may be unaffected by this specific bypass.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 4 November 2026; the vendor's advisory wins where it differs.
- The sections headed "The bottom line", "Does this apply to you?", "What it is", "Why it matters", "Exposure by situation", "Things people will get wrong", "How we would triage it" and "Send this to your IT provider" are our interpretation of the sources, not a statement by CISA or the vendor.

Appendix 1. Severity decoded

CVE-2024-27834: score 5.5, `CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N` As the CVE record gives it. The record's own score can differ from the base score on the NVD record.

Metric	Value	What it means here
Attack vector	Local	Needs an account or code already running on the machine.
Attack complexity	Low	No special conditions beyond the flaw itself.
Privileges required	Low	An ordinary account is enough.
User interaction	None	No one has to do anything.
Scope	Unchanged	Damage stays inside the vulnerable component.
Confidentiality	None	No data exposed.
Integrity	High	Total loss of integrity.
Availability	None	No effect on availability.

Appendix 2. Timeline

Date	Event
13 May 2024	CVE record published by Apple.
4 November 2026	CISA added it to its list of exploited vulnerabilities.
18 November 2026	CISA's deadline for US federal agencies.

Appendix 3. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

Your situation	Priority	Timeframe
iPhone or iPad below iOS/iPadOS 17.5 (or 16.7.8) used to browse the web	High	Within CISA's window — by 18 November 2026
Mac running macOS below Sonoma 14.5 or Safari below 17.5	High	Within CISA's window — by 18 November 2026
Organisation-managed Apple device fleet with deferred software updates enabled	High	This week — verify update compliance before the deadline

Apple TV running tvOS below 17.5 or Apple Watch running watchOS below 10.5	Medium	This patch cycle
Apple devices already at or above the fixed versions	None	None for this CVE

Appendix 4. Definition of done

- Every Apple Multiple Products you run is listed, with its version.
- Each is outside the affected list, or the vendor's mitigation is in place.
- The version output or a screenshot is saved with the date.
- Your projects' declared dependencies were checked against this CVE, and every row has a written reason.
- Logs for the weeks before the update were searched, and anything odd was written down.
- Anything not done has an owner and a date.

Sources

- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- CVE record for CVE-2024-27834: https://www.cve.org/CVERecord?id=CVE-2024-27834
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Advisory or release notes read: support.apple.com/en-us/120896: https://support.apple.com/en-us/120896
- Advisory or release notes read: support.apple.com/en-us/120898: https://support.apple.com/en-us/120898
- Advisory or release notes read: support.apple.com/en-us/120902: https://support.apple.com/en-us/120902
- Reference in the CVE record: support.apple.com: https://support.apple.com/en-us/120901
- Reference in the CVE record: support.apple.com: https://support.apple.com/en-us/120903