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

Any organisation managing Apple iPhones, iPads, Macs, Apple TVs, or Apple Watches should update all affected devices to the fixed releases before 18 November 2026. Check which devices are still below …

PREPARED BY	NamiQ	DATE	7 November 2026
FACTS AS OF	7 November 2026	VERSION	1.0
SEVERITY	**Medium: CVSS 3.1 5.5**	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

> *Any organisation managing Apple iPhones, iPads, Macs, Apple TVs, or Apple Watches should update all affected devices to the fixed releases before 18 November 2026. Check which devices are still below the fixed versions and prioritise those used for web browsing.*

At a glance

Fact	Detail
Product	Apple Multiple Products (CVE-2024-27834)
Severity	Medium: 5.5 (CVSS 3.1)
CISA	On its exploited list since 4 November 2026. Deadline for US federal agencies: 18 November 2026.
Chance of exploitation (EPSS)	0.02, the estimated chance in the next 30 days, as at 7 November 2026
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	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).
Who looks first	Administrators responsible for Apple devices running iOS, iPadOS, macOS, Safari, tvOS, or watchOS on versions the CVE record lists as affected — most urgent for devices used regularly for web browsing.

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 devices — iPhone, iPad, Mac, Apple TV, or Apple Watch?	Nothing to do for this CVE.	Check the software version on each device.
Are any of those devices running software older than the fixed versions listed above?	Already patched; no further action needed.	Update each affected device to the fixed release.
Were any unpatched devices used for web browsing or exposed to untrusted content before updating?	Patch and monitor; risk of prior exposure is lower.	Patch immediately and review the look-for section below.

What it is

An attacker who already has arbitrary read and write access on the device can use this flaw to bypass Pointer Authentication, a hardware mechanism designed to prevent memory-corruption exploits from becoming reliable code execution.

Why it matters

Pointer Authentication (PAC) is a hardware defence against forging code or data pointers — a key barrier between a memory-corruption primitive and full device compromise. An attacker who already has arbitrary read and write capability can use this flaw to bypass PAC and convert that primitive into reliable code execution. The CVSS of 5.5 reflects the prerequisite that such access must exist first. The CISA listing confirms active exploitation. Our reading is that the low score understates operational value: a PAC bypass turns a difficult exploit into a reliable one, and the same update fixes multiple WebKit memory-corruption flaws that could supply the required read/write access.

What the vendor's advisory says

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

- Safari 17.5 also fixed CVE-2024-27833 (WebKit integer overflow, code execution), CVE-2024-27856 (WebKit, code execution from a file), and CVE-2024-27820 (WebKit Web Inspector, code execution). No CVSS scores are given in the advisory for these.
- The same release also fixed fingerprinting issues CVE-2024-27838, CVE-2024-27850, CVE-2024-27830 (WebKit Canvas), and CVE-2024-27844 (Safari permission dialog persisting after navigation).
- The advisory does not describe a workaround for CVE-2024-27834; updating to the fixed version is the only remediation listed.

Things people will get wrong

- The CVSS 5.5 score means this is low priority. The score reflects the prerequisite of existing arbitrary R/W access. CISA's listing confirms active exploitation, so patching is required regardless of the score.
- Only devices already fully compromised are at risk. The same update fixes multiple WebKit memory-corruption flaws that could supply the read/write primitive this bypass needs. The two classes of flaw are addressed together.

How we would triage it

This is our judgement.

Step 1: Find the software versions on each Apple device

- On iPhone or iPad: Settings → General → About → Software Version. Compare against iOS 16.7.8 (older devices) or iOS 17.5.
- On Mac: Apple menu → About This Mac. The fixed macOS version is Sonoma 14.5.
- On Apple TV: Settings → System → Software Updates. On Apple Watch: Settings → General → Software Update. Fixed versions are tvOS 17.5 and watchOS 10.5.

Step 2: Update each device to the fixed release

- iOS and iPadOS: Settings → General → Software Update. Install iOS 16.7.8 (older devices) or iOS 17.5.
- macOS: System Settings → General → Software Update. Install macOS Sonoma 14.5 or later.
- Safari on macOS Monterey or Ventura: update Safari separately to 17.5 via System Settings → Software Update.

Step 3: Confirm versions after each update

- Re-check the version on each device to confirm the fixed release is in place.
- On macOS, Safari menu → About Safari should report version 17.5 or later.

Step 4: Review devices that browsed the web before patching

- If any device was used for web browsing while on an affected version, check for the signs listed in the look-for section.
- Consider whether a device management policy can enforce automatic updates to prevent recurrence.

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 about CVE-2024-27834, a Pointer Authentication bypass affecting Apple Safari, iOS, iPadOS, macOS, tvOS, and watchOS. CISA has listed it with a remediation deadline of 18 November 2026. Could you please check which of our Apple devices are running software older than the fixed versions — Safari 17.5, iOS 16.7.8 or 17.5, iPadOS 16.7.8 or 17.5, macOS Sonoma 14.5, tvOS 17.5, and watchOS 10.5 — and arrange for those to be updated? We would like written confirmation of the current version on each device and that the update has been applied before 18 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:

- Repeated unexpected crashes of Safari or WebKit-based apps on a device that browsed untrusted web content while running an affected version.
- Unfamiliar background processes or new device management profiles on iOS or macOS devices that were on affected versions during regular web use.

The weakness behind it

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

Likely ATT&CK mapping

MITRE ATT&CK is a public catalogue of the steps attackers take, from getting in to causing damage. No source has mapped this flaw to it yet, so the steps below are our prediction from what the record says the flaw allows. They are not MITRE's, the vendor's or CISA's, and an attacker may do other things.

Steps an attacker would likely take with this flaw

The step, in plain words	Stage of an attack	Why we think so
Exploitation for Client Execution (T1203): Making a program run the attacker's code by exploiting a flaw in software a person opens.	Execution: running the attacker's code	If the read/write capability was obtained via a WebKit memory-corruption flaw triggered by visiting a webpage, exploitation for client execution via web content would typically be the delivery path.

Exploitation for Privilege Escalation (T1068): Using a flaw to gain higher rights than the account had, such as administrator or root.	Privilege Escalation: gaining higher rights	PAC bypass converts an existing arbitrary R/W primitive into reliable code execution; this would typically be used to escalate privileges within the process or sandbox.

How to use this: ask your IT provider which control or log would show each step, for example whether sign-in attempts from the internet are recorded. If nobody can answer, that is the gap to close first.

MITRE ATT&CK® is a registered trademark of The MITRE Corporation. Technique names are MITRE's.

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 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-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. 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

- The CVE record does not list watchOS in its affected-products table, though the CISA description and Apple advisory text both include it; the discrepancy is not explained.
- No workaround is described in the advisory for environments that cannot immediately update.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 7 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", "Likely ATT&CK mapping", "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 on iOS/iPadOS before 16.7.8 or 17.5, used for web browsing	High	Before 18 November 2026
Mac running macOS Sonoma before 14.5, with Safari or any WebKit-based browser	High	Before 18 November 2026
Apple TV on tvOS before 17.5 or Apple Watch on watchOS before 10.5	Medium	This week

All affected devices already updated to the fixed versions	None	No action needed 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