CVE-2024-27834

Apple Multiple Products Improper Authentication Vulnerability

CISA KEV since Nov 4, 2026 | Actively exploited

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.

EVRS	CVSS V3.1	EPSS	CISA DEADLINE
75/100	5.5	0.006	Nov 18, 2026
Urgent priority	Medium · NVD	48.8th percentile · FIRST	CISA federal deadline in 13 days

Signals behind the score

counted in the score | not counted — evidence for 6 of 8 signals

✓ **CISA KEV**	Listed in the catalog	− **Vendor exploitation**	Confirmed exploitation in the wild
− **Ransomware**	No known ransomware campaign association	✓ **KEV recency**	Added to CISA KEV within the last 30 days
✓ **EPSS**	0.006 probability	− **Pre-patch disclosure**	Disclosure status unavailable
✓ **CVSS**	Base score 5.5	− **Microsoft Exploitability Index**	Not a Microsoft CVE

Remediation

Patch This Cycle — Patch or fixed version identified

CISA required action: Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes). Follow applicable BOD 26-04 guidance for cloud services or discontinue use of the product if mitigations are unavailable. Stakeholders are responsible for evaluating each asset's internet exposure and ensuring adherence to BOD 26-04 patching guidelines.

Basis: CISA KEV required action

Affected and fixed versions · 1 more affected product on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
safari	< 17.5	no fixed version listed	NVD
webkitgtk	< 2.44.2	no fixed version listed	NVD
wpe webkit	< 2.44.2	no fixed version listed	NVD
ipados	< 17.5	no fixed version listed	NVD
iphone os	< 17.5	no fixed version listed	NVD
macos	⩾ 14.0 < 14.5	no fixed version listed	NVD
tvos	< 17.5	no fixed version listed	NVD
watchos	< 10.5	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-4rmp-jjj9-cfm4	**support.apple.com**	support.apple.com/en-us/120896
support.apple.com	support.apple.com/en-us/120898	**support.apple.com**	support.apple.com/en-us/120901
support.apple.com	support.apple.com/en-us/120902	**support.apple.com**	support.apple.com/en-us/120903
support.apple.com	support.apple.com/en-us/120905	**BOD 26-04**	cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk
Forensics Triage Requirements	cisa.gov/news-events/directives/bod-26-04-implementation-guidance-prioritizing-security-updates-based-risk	**NVD**	nvd.nist.gov/vuln/detail/CVE-2024-27834
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	**ENISA EUVD**	euvd.enisa.europa.eu/vulnerability/EUVD-2024-25027
Current data	evulnable.com/vulnerability-management/cve/CVE-2024-27834		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.