

CVE-2025-24085

Apple Multiple Products Use-After-Free Vulnerability

CISA KEV since Jan 29, 2025

Actively exploited

A use after free issue was addressed with improved memory management. This issue is fixed in iOS 18.3 and iPadOS 18.3, iPadOS 17.7.6, macOS Sequoia 15.3, macOS Sonoma 14.7.5, macOS Ventura 13.7.5, tvOS 18.3, visionOS 2.3, watchOS 11.3. A malicious application may be able to elevate privileges. Apple is aware of a report that this issue may have been actively exploited against versions of iOS before iOS 17.2.

EVRS 75 _{/100} Urgent priority	CVSS V3.1 10.0 Critical · NVD	EPSS 0.175 97.1st percentile · FIRST	CISA DEADLINE Feb 19, 2025 KEV since 2025 · listed over a year
--	--	---	---

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 two years
☒ EPSS	0.175 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 10.0	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified**CISA required action:** Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
ipados	< 17.7.6 ≥ 18.0 < 18.3	17.7.6 · 18.3	NVD
iphone os	< 18.3	18.3	NVD
macos	≥ 13.0 < 13.7.5 ≥ 14.0 < 14.7.5 ≥ 15.0 < 15.3	13.7.5 · 14.7.5 · 15.3	NVD
tvos	< 18.3	no fixed version listed	NVD
visionos	< 2.3	no fixed version listed	NVD
watchos	< 11.3	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-7h23-57pg-3hwc
support.apple.com support.apple.com/en-us/122068
support.apple.com support.apple.com/en-us/122072
NVD nvd.nist.gov/vuln/detail/CVE-2025-24085

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2025-3607

Additional guidance support.apple.com/en-us/122066
support.apple.com support.apple.com/en-us/122071
support.apple.com support.apple.com/en-us/122073
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnable.com/vulnerability-management/cve/CVE-2025-24085

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