

CVE-2023-41992

Apple Multiple Products Kernel Privilege Escalation Vulnerability

CISA KEV since Sep 25, 2023

Actively exploited

The issue was addressed with improved checks. This issue is fixed in macOS Monterey 12.7, iOS 16.7 and iPadOS 16.7, macOS Ventura 13.6. A local attacker may be able to elevate their privileges. Apple is aware of a report that this issue may have been actively exploited against versions of iOS before iOS 16.7.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 7.8 High · NVD	EPSS 0.095 95.4th percentile · FIRST	CISA DEADLINE Oct 16, 2023 KEV since 2023 · 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	On the CISA KEV catalog for over two years
☒ EPSS	0.095 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.8	☐ 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	< 16.7 17.0	16.7	NVD
iphone os	< 16.7 17.0	16.7	NVD
macos	≥ 12.0 < 12.7 ≥ 13.0 < 13.6	12.7 · 13.6	NVD

Sources

Vendor guidance support.apple.com	github.com/advisories/GHSA-wcch-rmq-7x86 support.apple.com/en-us/HT213926 , https://support.apple.com/en-us/HT213927 , https://support.apple.com/en-us/HT213928 , https://support.apple.com/en-us/HT213929 , https://support.apple.com/en-us/HT213931 , https://support.apple.com/en-us/HT213932	Additional guidance NVD	support.apple.com/en-us/HT213927 nvd.nist.gov/vuln/detail/CVE-2023-41992
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2023-46451
Current data	evulnable.com/vulnerability-management/cve/CVE-2023-41992		

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