

CVE-2024-23225

Apple Multiple Products Memory Corruption Vulnerability

CISA KEV since Mar 6, 2024

Actively exploited

A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 16.7.6 and iPadOS 16.7.6, iOS 17.4 and iPadOS 17.4, macOS Monterey 12.7.4, macOS Sonoma 14.4, macOS Ventura 13.6.5, tvOS 17.4, visionOS 1.1, watchOS 10.4. An attacker with arbitrary kernel read and write capability may be able to bypass kernel memory protections. Apple is aware of a report that this issue may have been exploited.

EVRS 75_{/100} Urgent priority	CVSS V3.1 7.8 High · NVD	EPSS 0.015 73.7th percentile · FIRST	CISA DEADLINE Mar 27, 2024 KEV since 2024 · 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	0.015 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	< 16.7.6 ≥ 17.0 < 17.4	16.7.6 · 17.4	NVD
iphone os	< 16.7.6 ≥ 17.0 < 17.4	16.7.6 · 17.4	NVD
macos	≥ 12.0 < 12.7.4 ≥ 13.0 < 13.6.5 ≥ 14.0 < 14.4	12.7.4 · 13.6.5	NVD
tvos	< 17.4	no fixed version listed	NVD
visionos	< 1.1	no fixed version listed	NVD
watchos	< 10.4	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-7r4v-4jv2-pj5p	Additional guidance	support.apple.com/en-us/120880
support.apple.com	support.apple.com/en-us/HT214081 , https://support.apple.com/en-us/HT214082 , https://support.apple.com/en-us/HT214083 , https://support.apple.com/en-us/HT214084 , https://support.apple.com/en-us/HT214085 , https://support.apple.com/en-us/HT214086 , https://support.apple.com/en-us/HT214087 , https://support.apple.com/en-us/HT214088	NVD	nvd.nist.gov/vuln/detail/CVE-2024-23225
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2024-20744
Current data	evulnable.com/vulnerability-management/cve/CVE-2024-23225		

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