

CVE-2022-48618

Apple Multiple Products Memory Corruption Vulnerability

CISA KEV since Jan 31, 2024

Actively exploited

The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.1, watchOS 9.2, iOS 16.2 and iPadOS 16.2, tvOS 16.2. An attacker with arbitrary read and write capability may be able to bypass Pointer Authentication. Apple is aware of a report that this issue may have been exploited against versions of iOS released before iOS 15.7.1.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 7.0 High · NVD	EPSS 0.005 41st percentile · FIRST	CISA DEADLINE Feb 21, 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	0.005 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.0	☐ 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	< 16.2	16.2	NVD
iphone os	< 16.2	16.2	NVD
macos	≥ 13.0 < 13.1	13.1	NVD
tvos	< 16.2	16.2	NVD
watchos	< 9.2	9.2	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-v2rr-hhf4-8739	Additional guidance	support.apple.com/en-us/HT213530
support.apple.com	support.apple.com/en-us/HT213530 , https://support.apple.com/en-us/HT213532 , https://support.apple.com/en-us/HT213535 , https://support.apple.com/en-us/HT213536	NVD	nvd.nist.gov/vuln/detail/CVE-2022-48618
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2022-51313
Current data	evulnable.com/vulnerability-management/cve/CVE-2022-48618		

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