

CVE-2023-32434

Apple Multiple Products Integer Overflow Vulnerability

CISA KEV since Jun 23, 2023

Actively exploited

An integer overflow was addressed with improved input validation. This issue is fixed in watchOS 9.5.2, macOS Big Sur 11.7.8, iOS 15.7.7 and iPadOS 15.7.7, macOS Monterey 12.6.7, watchOS 8.8.1, iOS 16.5.1 and iPadOS 16.5.1, macOS Ventura 13.4.1. An app may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited against versions of iOS released before iOS 15.7.

EVRS 75_{/100} Urgent priority	CVSS V3.1 7.8 High · NVD	EPSS 0.515 98.9th percentile · FIRST	CISA DEADLINE Jul 14, 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	0.515 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 updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
ipados	< 15.7.7 ≥ 16.0 < 16.5.1	15.7.7 · 16.5.1	NVD
iphone os	< 15.7.7 ≥ 16.0 < 16.5.1	15.7.7 · 16.5.1	NVD
macos	≥ 11.0 < 11.7.8 ≥ 12.0.0 < 12.6.7 ≥ 13.0 < 13.4.1	11.7.8 · 12.6.7	NVD
watchos	< 8.8.1 ≥ 9.0 < 9.5.2	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-4pvh-jrgh-mpvj	Additional guidance	support.apple.com/en-us/HT213808
support.apple.com	support.apple.com/en-us/HT213808 , https://support.apple.com/en-us/HT213812 , https://support.apple.com/en-us/HT213809 , https://support.apple.com/en-us/HT213810 , https://support.apple.com/en-us/HT213813 , https://support.apple.com/en-us/HT213811 , https://support.apple.com/en-us/HT213814	NVD	nvd.nist.gov/vuln/detail/CVE-2023-32434
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2023-36678
Current data	evulnable.com/vulnerability-management/cve/CVE-2023-32434		

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