

CVE-2025-31200

Apple Multiple Products Memory Corruption Vulnerability

CISA KEV since Apr 17, 2025

Actively exploited

A memory corruption issue was addressed with improved bounds checking. This issue is fixed in iOS 18.4.1 and iPadOS 18.4.1, macOS Sequoia 15.4.1, tvOS 18.4.1, visionOS 2.4.1, watchOS 11.5. Processing an audio stream in a maliciously crafted media file may result in code execution. Apple is aware of a report that this issue may have been exploited in an extremely sophisticated attack against specific targeted individuals on versions of iOS released before iOS 18.4.1.

EVRS 75/₁₀₀ Urgent priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.209 97.6th percentile · FIRST	CISA DEADLINE May 8, 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	0.209 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
macos	≥ 15.0 < 15.4.1	15.4.1	NVD
tvos	< 18.4.1	18.4.1	NVD
visionos	< 2.4.1	2.4.1	NVD
ipados	< 18.4.1	18.4.1	NVD
iphone os	< 18.4.1	18.4.1	NVD
watchos	< 11.5	11.5	NVD

Sources

Vendor guidance github.com/advisories/GHSA-8f6m-fvf9-6397
support.apple.com support.apple.com/en-us/122400
support.apple.com support.apple.com/en-us/122402
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnable.com/vulnerability-management/cve/CVE-2025-31200

Additional guidance support.apple.com/en-us/122282
support.apple.com support.apple.com/en-us/122401
NVD nvd.nist.gov/vuln/detail/CVE-2025-31200
ENISA EUVD evvd.enisa.europa.eu/vulnerability/EUVD-2025-11380

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