

CVE-2023-41974

Apple iOS and iPadOS Use-After-Free Vulnerability

CISA KEV since Mar 5, 2026

Actively exploited

A use-after-free issue was addressed with improved memory management. This issue is fixed in iOS 17 and iPadOS 17, iOS 15.8.7 and iPadOS 15.8.7. An app may be able to execute arbitrary code with kernel privileges.

EVRS 75 _{/100} Urgent priority	CVSS V3.1 7.8 High · NVD	EPSS 0.020 80.1st percentile · FIRST	CISA DEADLINE Mar 26, 2026 CISA federal deadline · Overdue by 7 months
--	---------------------------------------	---	---

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 year
☒ EPSS	0.020 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, 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
ipados	< 15.8.7 ≥ 16.0 < 17.0	15.8.7 · 17.0	NVD
iphone os	< 15.8.7 ≥ 16.0 < 17.0	15.8.7 · 17.0	NVD

Sources

Vendor guidance github.com/advisories/GHSA-58c3-hjfx-2gmq
support.apple.com support.apple.com/en-us/HT213938
NVD nvd.nist.gov/vuln/detail/CVE-2023-41974

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2023-46433

Additional guidance support.apple.com/en-us/120949
support.apple.com support.apple.com/kb/HT213938
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnable.com/vulnerability-management/cve/CVE-2023-41974

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