

CVE-2023-41064

Apple iOS, iPadOS, and macOS ImageIO Buffer Overflow Vulnerability

CISA KEV since Sep 11, 2023

Actively exploited

A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 16.6.1 and iPadOS 16.6.1, macOS Monterey 12.6.9, macOS Ventura 13.5.2, iOS 15.7.9 and iPadOS 15.7.9, macOS Big Sur 11.7.10. Processing a maliciously crafted image may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.

EVRS 75_{/100} Urgent priority	CVSS V3.1 7.8 High · NVD	EPSS 0.534 99th percentile · FIRST	CISA DEADLINE Oct 2, 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	0.534 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	< 15.7.9 ≥ 16.0 < 16.6.1	15.7.9 · 16.6.1	NVD
iphone os	< 15.7.9 ≥ 16.0 < 16.6.1	15.7.9 · 16.6.1	NVD
macos	≥ 11.0 < 11.7.10 ≥ 12.0 < 12.6.9 ≥ 13.0 < 13.5.2	11.7.10 · 12.6.9	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-8c6q-gxj3-w77f	Additional guidance	support.apple.com/en-us/HT213905
support.apple.com	support.apple.com/en-us/HT213905 , https://support.apple.com/en-us/HT213906	NVD	nvd.nist.gov/vuln/detail/CVE-2023-41064
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2023-45585
Current data	evulnable.com/vulnerability-management/cve/CVE-2023-41064		

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