

CVE-2023-28205

Apple Multiple Products WebKit Use-After-Free Vulnerability

CISA KEV since Apr 10, 2023

Actively exploited

A use after free issue was addressed with improved memory management. This issue is fixed in Safari 16.4.1, iOS 15.7.5 and iPadOS 15.7.5, iOS 16.4.1 and iPadOS 16.4.1, macOS Ventura 13.3.1. Processing maliciously crafted web content 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 8.8 High · NVD	EPSS 0.271 98th percentile · FIRST	CISA DEADLINE May 1, 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	0.271 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.8	☐ 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
safari	< 16.4.1	no fixed version listed	NVD
ipados	< 15.7.5 ≥ 16.0 < 16.4.1	no fixed version listed	NVD
iphone os	< 15.7.5 ≥ 16.0 < 16.4.1	no fixed version listed	NVD
macos	< 13.3.1	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-6qjh-p74q-89mv

support.apple.com support.apple.com/en-us/HT213720, <https://support.apple.com/en-us/HT213721>, <https://support.apple.com/en-us/HT213722>, <https://support.apple.com/en-us/HT213723>

NVD nvd.nist.gov/vuln/detail/CVE-2023-28205

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2023-31913

Current data evulnable.com/vulnerability-management/cve/CVE-2023-28205

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