

CVE-2024-23222

Apple Multiple Products WebKit Type Confusion Vulnerability

CISA KEV since Jan 23, 2024

Actively exploited

A type confusion issue was addressed with improved checks. This issue is fixed in Safari 17.3, iOS 15.8.7 and iPadOS 15.8.7, iOS 16.7.5 and iPadOS 16.7.5, iOS 17.3 and iPadOS 17.3, macOS Monterey 12.7.3, macOS Sonoma 14.3, macOS Ventura 13.6.4, tvOS 17.3, visionOS 1.0.2. Processing maliciously crafted web content may lead to arbitrary code execution. This fix associated with the Coruna exploit was shipped in iOS 17.3 on January 22, 2024. This update brings that fix to devices that cannot update to the latest iOS version.

EVRS 75/₁₀₀ Urgent priority	CVSS V3.1 8.8 High · NVD	EPSS 0.106 95.8th percentile · FIRST	CISA DEADLINE Feb 13, 2024 KEV since 2024 · 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	0.106 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 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
safari	< 17.3	no fixed version listed	NVD
ipados	< 15.8.7 ≥ 16.0 < 16.7.5 ≥ 17.0 < 17.3	no fixed version listed	NVD
iphone os	< 15.8.7 ≥ 16.0 < 16.7.5 ≥ 17.0 < 17.3	no fixed version listed	NVD
macos	≥ 12.0 < 12.7.3 ≥ 13.0 < 13.6.4 ≥ 14.0 < 14.3	no fixed version listed	NVD
tvos	< 17.3	no fixed version listed	NVD
visionos	< 1.0.2	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-93px-8x98-j7p2	Additional guidance	support.apple.com/en-us/118479
support.apple.com	support.apple.com/en-us/HT214055 , https://support.apple.com/en-us/HT214056 , https://support.apple.com/en-us/HT214057 , https://support.apple.com/en-us/HT214058 , https://support.apple.com/en-us/HT214059 , https://support.apple.com/en-us/HT214061 , https://support.apple.com/en-us/HT214063	NVD	nvd.nist.gov/vuln/detail/CVE-2024-23222
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2024-20741
Current data	evulnable.com/vulnerability-management/cve/CVE-2024-23222		

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