

CVE-2024-44309

Apple Multiple Products Cross-Site Scripting (XSS) Vulnerability

CISA KEV since Nov 21, 2024

Actively exploited

A cookie management issue was addressed with improved state management. This issue is fixed in Safari 18.1.1, iOS 17.7.2 and iPadOS 17.7.2, iOS 18.1.1 and iPadOS 18.1.1, macOS Sequoia 15.1.1, visionOS 2.1.1. Processing maliciously crafted web content may lead to a cross site scripting attack. Apple is aware of a report that this issue may have been actively exploited on Intel-based Mac systems.

EVRS 75/₁₀₀ Urgent priority	CVSS V3.1 6.3 Medium · NVD	EPSS 0.226 97.7th percentile · FIRST	CISA DEADLINE Dec 12, 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	Added to CISA KEV within the last two years
☒ EPSS	0.226 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 6.3	☐ 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	< 18.1.1	no fixed version listed	NVD
debian linux	11.0	no fixed version listed	NVD
ipados	< 17.7.2 ≥ 18.0 < 18.1.1	no fixed version listed	NVD
iphone os	< 17.7.2 ≥ 18.0 < 18.1.1	no fixed version listed	NVD
macos	≥ 15.0 < 15.1.1	no fixed version listed	NVD
visionos	< 2.1.1	no fixed version listed	NVD

Sources

Vendor guidance support.apple.com/en-us/121752

support.apple.com support.apple.com/en-us/121752, <https://support.apple.com/en-us/121753>, <https://support.apple.com/en-us/121754>, <https://support.apple.com/en-us/121755>, <https://support.apple.com/en-us/121756>

NVD nvd.nist.gov/vuln/detail/CVE-2024-44309

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

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2024-41208

Current data evulnable.com/vulnerability-management/cve/CVE-2024-44309

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