

CVE-2022-32893

Apple iOS and macOS Out-of-Bounds Write Vulnerability

CISA KEV since Aug 18, 2022

Actively exploited

An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 15.6.1 and iPadOS 15.6.1, macOS Monterey 12.5.1, Safari 15.6.1. 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 0.099 95.6th percentile · FIRST	CISA DEADLINE Sep 8, 2022 KEV since 2022 · 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	0.099 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	< 15.6.1	no fixed version listed	NVD
webkitgtk	< 2.36.7	no fixed version listed	NVD
wpe webkit	< 2.36.7	no fixed version listed	NVD
ipados	< 15.6.1	no fixed version listed	NVD
iphone os	< 15.6.1	no fixed version listed	NVD
macos	≥ 12.0 < 12.5.1	no fixed version listed	NVD
fedora	35 36	no fixed version listed	NVD
debian linux	10.0 11.0	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-qjpw-c5xf-g33j
support.apple.com support.apple.com/en-gb/HT213412, <https://support.apple.com/en-gb/HT213413>
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnable.com/vulnerability-management/cve/CVE-2022-32893

Additional guidance support.apple.com/en-us/HT213412
NVD nvd.nist.gov/vuln/detail/CVE-2022-32893
ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2022-35959

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