

CVE-2021-30900

Apple iOS, iPadOS, and macOS Out-of-Bounds Write Vulnerability

CISA KEV since Mar 30, 2023

Actively exploited

An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 14.8.1 and iPadOS 14.8.1, iOS 15.1 and iPadOS 15.1. A malicious application may be able to execute arbitrary code with kernel privileges.

EVRS 75 _{/100} Urgent priority	CVSS V3.1 7.8 High · NVD	EPSS 0.052 92.5th percentile · FIRST	CISA DEADLINE Apr 20, 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	0.052 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 updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
ipados	< 14.8.1 15.0	14.8.1	NVD
iphone os	< 14.8.1 15.0	14.8.1	NVD
macos	< 11.6.1	11.6.1	NVD

Sources

Vendor guidance support.apple.com/en-us/HT212867**support.apple.com** support.apple.com/en-us/HT212866, <https://support.apple.com/en-us/HT212868>, <https://support.apple.com/kb/HT212872>**NVD** nvd.nist.gov/vuln/detail/CVE-2021-30900**CISA KEV** cisa.gov/known-exploited-vulnerabilities-catalog**ENISA EUVD** euvd.enisa.europa.eu/vulnerability/EUVD-2021-17817**Current data** evulnable.com/vulnerability-management/cve/CVE-2021-30900

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