

CVE-2022-22675

Apple macOS Out-of-Bounds Write Vulnerability

CISA KEV since Apr 4, 2022

Actively exploited

An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in tvOS 15.5, watchOS 8.6, macOS Big Sur 11.6.6, macOS Monterey 12.3.1, iOS 15.4.1 and iPadOS 15.4.1. An application may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited..

EVRS 75 _{/100} Urgent priority	CVSS V3.1 7.8 High · NVD	EPSS 0.125 96.2nd percentile · FIRST	CISA DEADLINE Apr 25, 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	0.125 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	< 15.4.1	15.4.1	NVD
iphone os	< 15.4.1	15.4.1	NVD
macos	≥ 11.0 < 11.6.6 ≥ 12.0.0 < 12.3.1	11.6.6 · 12.3.1	NVD
tvos	< 15.5	15.5	NVD
watchos	< 8.6	8.6	NVD

Sources

Vendor guidance github.com/advisories/GHSA-xj88-rf28-xgv9
NVD nvd.nist.gov/vuln/detail/CVE-2022-22675**ENISA EUVD** euvd.enisa.europa.eu/vulnerability/EUVD-2022-27820**Additional guidance** support.apple.com/en-us/HT213219
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnable.com/vulnerability-management/cve/CVE-2022-22675

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