

CVE-2022-22587

Apple Memory Corruption Vulnerability

CISA KEV since Jan 28, 2022

Actively exploited

A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 15.3 and iPadOS 15.3, macOS Big Sur 11.6.3, macOS Monterey 12.2. A malicious 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 9.8 Critical · NVD	EPSS 0.116 96.1st percentile · FIRST	CISA DEADLINE Feb 11, 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	0.116 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ 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	< 15.3	15.3	NVD
iphone os	< 15.3	15.3	NVD
macos	< 11.6.3 ≥ 12.0 < 12.2	11.6.3 · 12.2	NVD

Sources

Vendor guidance github.com/advisories/GHSA-p75p-vc6x-p9wf
NVD nvd.nist.gov/vuln/detail/CVE-2022-22587

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2022-27732

Additional guidance support.apple.com/en-us/HT213053
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnable.com/vulnerability-management/cve/CVE-2022-22587

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