

CVE-2022-22674

Apple macOS Out-of-Bounds Read Vulnerability

CISA KEV since Apr 4, 2022

Actively exploited

An out-of-bounds read issue existed that led to the disclosure of kernel memory. This was addressed with improved input validation. This issue is fixed in macOS Monterey 12.3.1, Security Update 2022-004 Catalina, macOS Big Sur 11.6.6. A local user may be able to read kernel memory.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 5.5 Medium · NVD	EPSS 0.011 65th 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	0.011 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 5.5	☐ 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
mac os x	≥ 10.15 < 10.15.7 10.15.7	10.15.7	NVD
macos	≥ 11.0 < 11.6.6 ≥ 12.0.0 < 12.3.1	11.6.6 · 12.3.1	NVD

Sources

Vendor guidance	support.apple.com/en-us/HT213220	NVD	nvd.nist.gov/vuln/detail/CVE-2022-22674
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2022-27819
Current data	evulnable.com/vulnerability-management/cve/CVE-2022-22674		

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