

CVE-2019-8526

Apple macOS Use-After-Free Vulnerability

CISA KEV since Apr 17, 2023

Actively exploited

A use after free issue was addressed with improved memory management. This issue is fixed in macOS Mojave 10.14.4. An application may be able to gain elevated privileges.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 7.8 High · NVD	EPSS 0.007 52.7th percentile · FIRST	CISA DEADLINE May 8, 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	0.007 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
mac os x	< 10.14.4	10.14.4	NVD

Sources

Vendor guidance github.com/advisories/GHSA-p8m9-gxw7-g5pf
support.apple.com support.apple.com/en-us/HT209600
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnable.com/vulnerability-management/cve/CVE-2019-8526

Additional guidance support.apple.com/HT209600
NVD nvd.nist.gov/vuln/detail/CVE-2019-8526
ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2019-17916

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