

CVE-2020-9934

Apple iOS, iPadOS, and macOS Input Validation Vulnerability

CISA KEV since Sep 8, 2022

Actively exploited

Public exploit module (Metasploit)

An issue existed in the handling of environment variables. This issue was addressed with improved validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6. A local user may be able to view sensitive user information.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 5.5 Medium · NVD	EPSS 0.032 88.1st percentile · FIRST	CISA DEADLINE Sep 29, 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	0.032 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
ipados	< 13.6	13.6	NVD
iphone os	< 13.6	13.6	NVD
mac os x	< 10.15.6	10.15.6	NVD

Sources

Vendor guidance support.apple.com/HT211288**support.apple.com** support.apple.com/en-us/HT211288, <https://support.apple.com/en-us/HT211289>**NVD** nvd.nist.gov/vuln/detail/CVE-2020-9934**CISA KEV** cisa.gov/known-exploited-vulnerabilities-catalog**ENISA EUVD** euvd.enisa.europa.eu/vulnerability/EUVD-2020-30713**Current data** evulnable.com/vulnerability-management/cve/CVE-2020-9934

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