

CVE-2020-27932

Apple Multiple Products Type Confusion Vulnerability

CISA KEV since Nov 3, 2021

Actively exploited

A type confusion issue was addressed with improved state handling. This issue is fixed in macOS Big Sur 11.0.1, watchOS 7.1, iOS 12.4.9, watchOS 6.2.9, Security Update 2020-006 High Sierra, Security Update 2020-006 Mojave, iOS 14.2 and iPadOS 14.2, watchOS 5.3.9, macOS Catalina 10.15.7 Supplemental Update, macOS Catalina 10.15.7 Update. A malicious application may be able to execute arbitrary code with kernel privileges.

EVRS 75 _{/100} Urgent priority	CVSS V3.1 7.8 High · NVD	EPSS 0.103 95.7th percentile · FIRST	CISA DEADLINE May 3, 2022 KEV since 2021 · 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	0.103 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
icloud	< 11.5	11.5	NVD
itunes	< 12.11	12.11	NVD
ipados	< 14.2	14.2	NVD
iphone os	< 12.4.9 ≥ 14.0 < 14.2	12.4.9 · 14.2	NVD
mac os x	< 10.15.7	10.15.7	NVD
macos	≥ 11.0 < 11.0.1	no fixed version listed	NVD
watchos	< 5.3.9 ≥ 6.0 < 6.2.9 ≥ 7.0 < 7.1	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-f3wv-rx3x-v6fh
NVD nvd.nist.gov/vuln/detail/CVE-2020-27932**ENISA EUVD** euvd.enisa.europa.eu/vulnerability/EUVD-2020-20425**Additional guidance** support.apple.com/en-us/HT211928
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnable.com/vulnerability-management/cve/CVE-2020-27932

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