CVE-2020-9907

Apple Multiple Products Memory Corruption Vulnerability

CISA KEV since Jun 27, 2022 | Actively exploited

A memory corruption issue was addressed by removing the vulnerable code. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8. An application may be able to execute arbitrary code with kernel privileges.

EVRS	CVSS V3.1	EPSS	CISA DEADLINE
75/100	7.8	0.032	Jul 18, 2022
Urgent priority	High · NVD	88th percentile · FIRST	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 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
ipados	< 13.6	13.6	NVD
iphone os	< 13.6	13.6	NVD
tvos	< 13.4.8	13.4.8	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-x2gp-c4cv-7chc	Additional guidance	support.apple.com/HT211288
NVD	nvd.nist.gov/vuln/detail/CVE-2020-9907	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2020-30686	Current data	evulnable.com/vulnerability-management/cve/CVE-2020-9907

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