CVE-2019-7287

Apple iOS Memory Corruption Vulnerability

CISA KEV since May 23, 2022 | Actively exploited

A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 12.1.4. An application may be able to execute arbitrary code with kernel privileges.

EVRS	CVSS V3.1	EPSS	CISA DEADLINE
75/100	7.8	0.046	Jun 13, 2022
Urgent priority	High · NVD	91.6th 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	0.046 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
iphone os	< 12.1.4	12.1.4	NVD

Sources

Vendor guidance	support.apple.com/HT209520	NVD	nvd.nist.gov/vuln/detail/CVE-2019-7287
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2019-16831
Current data	evulnable.com/vulnerability-management/cve/CVE-2019-7287		

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