

CVE-2021-30860

Apple Multiple Products Integer Overflow Vulnerability

CISA KEV since Nov 3, 2021

Actively exploited

An integer overflow was addressed with improved input validation. This issue is fixed in Security Update 2021-005 Catalina, iOS 14.8 and iPadOS 14.8, macOS Big Sur 11.6, watchOS 7.6.2. Processing a maliciously crafted PDF may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.

EVRS 78 _{/100} Urgent priority	CVSS V3.1 7.8 High · NVD	EPSS 0.760 99.53rd percentile · FIRST	CISA DEADLINE Nov 17, 2021 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	0.760 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
xpdf	< 4.04	no fixed version listed	NVD
poppler	< 22.09.0	no fixed version listed	NVD
ipados	< 14.8	14.8	NVD
iphone os	< 12.5.5 ≥ 13.0 < 14.8	12.5.5 · 14.8	NVD
mac os x	≥ 10.15 < 10.15.7 10.15.7	10.15.7	NVD
macos	< 11.6	11.6	NVD
watchos	< 7.6.2	7.6.2	NVD

Sources

Vendor guidance	support.apple.com/en-us/HT212804	NVD	nvd.nist.gov/vuln/detail/CVE-2021-30860
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2021-17777
Current data	evulnable.com/vulnerability-management/cve/CVE-2021-30860		

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