

CVE-2023-41061

Apple iOS, iPadOS, and watchOS Wallet Code Execution Vulnerability

CISA KEV since Sep 11, 2023

Actively exploited

A validation issue was addressed with improved logic. This issue is fixed in watchOS 9.6.2, iOS 16.6.1 and iPadOS 16.6.1. A maliciously crafted attachment may result in arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 7.8 High · NVD	EPSS 0.044 91.3rd percentile · FIRST	CISA DEADLINE Oct 2, 2023 KEV since 2023 · 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	0.044 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 mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
ipados	< 16.6.1	16.6.1	NVD
iphone os	< 16.6.1	16.6.1	NVD
watchos	< 9.6.2	9.6.2	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-h6m5-xj4q-9xw4	Additional guidance	support.apple.com/en-us/HT213905
support.apple.com	support.apple.com/en-us/HT213905 , https://support.apple.com/kb/HT213907	NVD	nvd.nist.gov/vuln/detail/CVE-2023-41061
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2023-45582
Current data	evulnable.com/vulnerability-management/cve/CVE-2023-41061		

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