

CVE-2025-55177

Meta Platforms WhatsApp Incorrect Authorization Vulnerability

CISA KEV since Sep 2, 2025

Actively exploited

Incomplete authorization of linked device synchronization messages in WhatsApp for iOS prior to v2.25.21.73, WhatsApp Business for iOS v2.25.21.78, and WhatsApp for Mac v2.25.21.78 could have allowed an unrelated user to trigger processing of content from an arbitrary URL on a target's device. We assess that this vulnerability, in combination with an OS-level vulnerability on Apple platforms (CVE-2025-43300), may have been exploited in a sophisticated attack against specific targeted users.

EVRS 75_{/100} Urgent priority	CVSS V3.1 5.4 Medium · NVD	EPSS 0.047 91.8th percentile · FIRST	CISA DEADLINE Sep 23, 2025 KEV since 2025 · 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	Added to CISA KEV within the last two years
☒ EPSS	0.047 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 5.4	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
whatsapp	≥ 2.22.25.2 < 2.25.21.73 ≥ 2.22.25.2 < 2.25.21.78	2.25.21.73 · 2.25.21.78	NVD
whatsapp business	≥ 2.22.25.2 < 2.25.21.78	2.25.21.78	NVD

Sources

Vendor guidance github.com/advisories/GHSA-f7wf-m2qg-r9rx

Additional guidance facebook.com/security/advisories/cve-2025-55177

whatsapp.com whatsapp.com/security/advisories/2025/
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

NVD nvd.nist.gov/vuln/detail/CVE-2025-55177
ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2025-26214

Current data evulnable.com/vulnerability-management/cve/CVE-2025-55177

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