

CVE-2019-18426

Meta Platforms WhatsApp Cross-Site Scripting Vulnerability

CISA KEV since May 23, 2022

Actively exploited

A vulnerability in WhatsApp Desktop versions prior to 0.3.9309 when paired with WhatsApp for iPhone versions prior to 2.20.10 allows cross-site scripting and local file reading. Exploiting the vulnerability requires the victim to click a link preview from a specially crafted text message.

EVRS 76 / ₁₀₀ Urgent priority	CVSS V3.1 8.2 High · NVD	EPSS 0.679 99.32nd percentile · FIRST	CISA DEADLINE Jun 13, 2022 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	0.679 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.2	☐ 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
whatsapp	< 0.3.9309 < 2.20.10	0.3.9309 · 2.20.10	NVD

Sources

Vendor guidance	facebook.com/security/advisories/cve-2019-18426	NVD	nvd.nist.gov/vuln/detail/CVE-2019-18426
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	europa.eu/enisa/eu-vulnerability/EUVD-2019-8195
Current data	evulnabile.com/vulnerability-management/cve/CVE-2019-18426		

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