

CVE-2019-3568

Meta Platforms WhatsApp VOIP Stack Buffer Overflow Vulnerability

CISA KEV since Apr 19, 2022

Actively exploited

A buffer overflow vulnerability in WhatsApp VOIP stack allowed remote code execution via specially crafted series of RTCP packets sent to a target phone number. The issue affects WhatsApp for Android prior to v2.19.134, WhatsApp Business for Android prior to v2.19.44, WhatsApp for iOS prior to v2.19.51, WhatsApp Business for iOS prior to v2.19.51, WhatsApp for Windows Phone prior to v2.18.348, and WhatsApp for Tizen prior to v2.18.15.

EVRS 75_{/100} Urgent priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.301 98.2nd percentile · FIRST	CISA DEADLINE May 10, 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	0.301 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ 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
whatsapp	< 2.18.15 < 2.18.348 < 2.19.51 < 2.19.134	2.18.15 · 2.18.348 · 2.19.51 · 2.19.134	NVD
whatsapp business	< 2.19.44 < 2.19.51	2.19.44 · 2.19.51	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-cmw5-mm8g-r4fr	NVD	nvd.nist.gov/vuln/detail/CVE-2019-3568
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2019-13204
Current data	evulnable.com/vulnerability-management/cve/CVE-2019-3568		

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