مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in WhatsApp

Tracking #:432318901

Date:05-05-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Meta has patched two significant security vulnerabilities in WhatsApp that could enable remote attackers to execute arbitrary URLs on victims' devices or deliver disguised malware through spoofed file attachments.

TECHNICAL DETAILS:

WhatsApp has addressed two significant security vulnerabilities that could allow threat actors to execute malicious actions on user devices across mobile and desktop environments. These issues, disclosed in a 2026 advisory by Meta Platforms, impact integrations with Instagram Reels and the Windows desktop client.
The vulnerabilities could enable:

- Remote triggering of arbitrary URLs via crafted messages
- Execution of disguised malicious files on Windows systems

Although no active exploitation has been observed, the attack vectors are considered high-risk due to their potential for remote code execution and malware delivery.

1. **CVE-2026-23866 – Instagram Reels Arbitrary URL Execution (High Severity)**
   - Affected Platforms: WhatsApp for iOS (v2.25.8.0 through v2.26.15.72) and WhatsApp for Android (v2.25.8.0 through v2.26.7.10).
   - Description: Incomplete validation of media content paths in AI-rich response messages associated with Instagram Reels.
   - Impact: Remote attackers can supply malicious URLs that WhatsApp processes without proper sanitization. This can trigger OS-level custom URL scheme handlers, potentially launching external apps, executing commands, or directing users to phishing/malware sites.
   - Attack Vector: Crafted WhatsApp messages containing manipulated Instagram Reels elements. No user interaction beyond opening the message may be required in some scenarios.
2. **CVE-2026-23863 – Windows Attachment Spoofing via NUL Bytes (High Severity)**
   - Affected Platforms: WhatsApp for Windows builds prior to v2.3000.1032164386.258709.
   - Description: Improper handling of file names containing embedded NUL (null) bytes.
   - Impact: Attackers can craft attachments that appear as safe files (e.g., .pdf or .txt) in the WhatsApp interface. When opened, the NUL byte terminates the displayed name, causing the OS to interpret and execute the true file extension (e.g., .exe), delivering malware or ransomware.

RECOMMENDATIONS:

Immediate Actions

- Update WhatsApp on all platforms:
  - Mobile users via official app stores (iOS/Android)
  - Windows users to latest desktop client version
- Enforce patch compliance across enterprise-managed devices

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.whatsapp.com/security/advisories/2026