مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Remote Code Execution Vulnerability in WhatsApp for Windows

Tracking #:432317053

Date:09-04-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a high-severity vulnerability has been discovered in WhatsApp Desktop for Windows that allows remote attackers to execute arbitrary code by sending malicious file attachments.

TECHNICAL DETAILS:

A high-severity vulnerability has been discovered in WhatsApp Desktop for Windows that allows remote attackers to execute arbitrary code by sending malicious file attachments. Attackers can exploit this flaw by crafting deceptive files that appear benign (e.g., images) within WhatsApp but are executed as malicious code when opened. The vulnerability poses a serious risk to user systems, especially in group chat environments, where the impact may be multiplied across several recipients.

Technical Details

- **CVE ID:** CVE-2025-30401
- **Vulnerability Type:** File Attachment Spoofing / Remote Code Execution
- **Severity Level:** High
- **Impact:** Remote code execution, unauthorized access, potential data exfiltration
- **Attack Vector:** Remote (via WhatsApp message attachments)
- **Affected Versions:** WhatsApp Desktop for Windows v0.0.0 to v2.2450.5
- **Fixed In:** Version 2.2450.6

RECOMMENDATIONS:

- Update WhatsApp Desktop for Windows to the latest fixed version.
- Avoid opening attachments from untrusted or unexpected sources and Verify file extensions before opening.

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.facebook.com/security/advisories/cve-2025-30401