مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

WhatsApp Patches Zero-Click Vulnerability Exploited in Sophisticated Attacks

Tracking #:432317656

Date-01-09-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed WhatsApp has addressed a security vulnerability in its messaging apps for Apple iOS and macOS that it said may have been exploited in the wild in conjunction with a recently disclosed Apple flaw in targeted zero-day attacks.

TECHNICAL DETAILS:

WhatsApp has released security updates to address CVE-2025-55177, a critical vulnerability in WhatsApp for iOS and macOS platforms that could allow an unrelated user to trigger processing of arbitrary content on a target device through insufficient authorization of linked device synchronization messages. The flaw may have been exploited in the wild as part of a zero-click attack chain targeting high-profile individuals, in conjunction with CVE-2025-43300, an out-of-bounds write vulnerability in Apple's ImageIO framework.

Technical Details

- **CVE-2025-55177**
  - **Type:** Incomplete Authorization / Improper Access Control
  - **Impact:** Allows a remote attacker to trigger the processing of content from an **arbitrary URL** on the victim's device via linked device sync messages.
  - **Attack Vector:** Zero-click (no user interaction required).
  - **Severity:** CVSS 8.0 (CISA-ADP) / 5.4 (Meta)
  - **Exploitation:** Confirmed active exploitation in targeted attacks.
- **CVE-2025-43300**
  - **Type:** Out-of-Bounds Write (ImageIO framework)
  - **Impact:** Memory corruption when processing malicious images.
  - **Chain:** Used with CVE-2025-55177 to achieve remote code execution and persistence.

Attack Characteristics

- Zero-click delivery (requires no user interaction).
- Linked device synchronization abused to process malicious URLs.
- Exploit chain allows full device compromise and spyware installation.

RECOMMENDATIONS:

- Update WhatsApp to the latest version immediately.
- Update iPhone, iPad, or Mac to the latest software.
- If suspect compromise, perform a full factory reset of the device.
- Always turn on automatic updates for apps and operating system.

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/2025