



**NATIONAL
CSIRT CY**



WhatsApp Zero-Click exploit affecting iOS and macOS

01/09/2025

(CVE-2025-55177)

CONFIDENTIAL

The content of this document is intended solely for use by the natural or legal person to whom it is addressed. If you gain access to this document by mistake, you should be aware that any forwarding, copying or disclosure of its content to any other person is strictly prohibited, and you must inform the sender immediately.

Executive Summary

A vulnerability with a CVSS score of 8.0 has been disclosed regarding WhatsApp instances in iOS and macOS devices.

The flaw allows a malicious actor to target unrelated victims to process content from an arbitrary url.

The vulnerability is zero click which means that the exploit does not require user interaction.

This vulnerability has been discovered by researchers within the WhatsApp security team.

WhatsApp recommends users to maintain their operating systems up to date.

Affected Products

- WhatsApp for iOS version 2.25.21.73
- WhatsApp Business for iOS version 2.25.21.78
- WhatsApp for Mac version 2.25.21.78

Common Vulnerabilities & Exposures

<https://nvd.nist.gov/vuln/detail/CVE-2025-55177>

Solutions

Make sure your apple devices operating systems as well as WhatsApp are updated to the latest versions.

Please distribute this information among your subsidiaries and partners, and also share with us any pertinent information and findings you may have (e.g IOCs, TTPs etc)

The Digital Security Authority extends its appreciation for the continued collaboration.

Disclaimer

Organizations are advised to consult with relevant cybersecurity professionals and follow best practices for their specific environments.