Computer Emergency Response Team of Mauritius
Ministry of Information Technology, Communication and Innovation

CERT-MU Vulnerability Note

WhatsApp fixes vulnerability used in zero-click attacks

Vulnerability Note: VN-2025-22

Date of Issue: 02 September 2025

Severity Rating: High

Systems Affected:

- WhatsApp for iOS prior to v2.25.21.73
- WhatsApp Business for iOS v2.25.21.78
- WhatsApp for Mac v2.25.21.78

Description

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. The vulnerability (CVE-2025-55177) relates to a case of insufficient authorization of linked device synchronization messages and could allow an unrelated user to trigger processing of content from an arbitrary URL on a target's device.

It also assessed that the shortcoming may have been chained with CVE-2025-43300, a vulnerability affecting iOS, iPadOS, and macOS, as part of a sophisticated attack against specific targeted users. CVE-2025-43300 was disclosed by Apple last week as having been weaponized in an extremely sophisticated attack against specific targeted individuals. The vulnerability in question is an out-of-bounds write vulnerability in the ImageIO framework that could result in memory corruption when processing a malicious image.

CVE Information
CVE-2025-43300
CVE-2025-55177

Mitigation
WhatsApp has recommended performing a full device factory reset and keeping their operating system and the WhatsApp app up-to-date for optimal protection.

Postal address
Mauritian Computer Emergency Response Team (CERT-MU)
Ministry of Information Technology, Communication and Innovation
2nd Floor, Wing A,
Shri Atal Bihari Vajpayee Tower,

Cybercity Ebene