Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CVE-2025-55177: WhatsApp Zero-Click Flaw Used in Targeted Campaigns

Date of Publication	Admiralty Code	TA Number
September 4, 2025	A1	TA2025268

Summary

Discovered On: August 2025
Affected Product: WhatsApp
Impact: A recently patched Zero-click flaw in WhatsApp's iOS and macOS apps, tracked as CVE-2025-55177, was exploited in targeted zero-day attacks as part of a sophisticated exploit chain with Apple's CVE-2025-43300. The WhatsApp bug allowed attackers to trick devices into processing malicious content, which was then combined with Apple's OS-level weakness to compromise specific high-value targets. Fewer than 200 users were notified of being targeted, but both WhatsApp and Apple confirmed the vulnerabilities were actively abused. Users are strongly urged to update WhatsApp and their devices immediately to stay protected.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-55177	Meta Platforms WhatsApp Incorrect Authorization Vulnerability	WhatsApp	✗	✓	✓
CVE-2025-43300	Apple iOS, iPadOS, and macOS Out-of-Bounds Write Vulnerability	Apple iOS, iPadOS, and macOS	✓	✓	✓

Vulnerability Details

#1

WhatsApp has rolled out patches for a security flaw in its iOS and macOS messaging clients that had been exploited in targeted zero-day attacks. Tracked as CVE-2025-55177, the bug stemmed from incomplete authorization in the handling of linked device synchronization messages. Left unpatched, it could have allowed an unrelated attacker to force the processing of content from an arbitrary URL on a victim's device, putting users at risk. The issue affected specific versions of WhatsApp for iOS, WhatsApp Business, and WhatsApp for Mac.

#2 What made this vulnerability especially dangerous is that it was not used alone. Instead, it acted as the entry point for a second and more severe flaw: Apple's **CVE-2025-43300**. It is said that adversaries chained the two vulnerabilities together, exploiting the WhatsApp bug to gain a foothold before leveraging Apple's OS-level weakness to escalate the attack. This kind of exploit chaining reflects the growing sophistication of targeted operations against high-value individuals.

#3 WhatsApp has confirmed that fewer than 200 users worldwide were targeted in this campaign and has sent in-app threat notifications to those affected. Both WhatsApp and Apple acknowledged that the flaws were being actively exploited in the wild.

#4 To contain the threat, WhatsApp advised impacted individuals to perform a full factory reset of their devices, alongside updating both the WhatsApp app and their operating system. The company has since issued updates that patch the vulnerability, making it critical for all users, whether targeted or not, to upgrade to the latest versions without delay.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-55177	WhatsApp for iOS prior to v2.25.21.73, WhatsApp Business for iOS v2.25.21.78, WhatsApp for Mac v2.25.21.78	cpe:2.3:a:whatsapp:whatsapp:*:*:*:*:*:*:iphone_os:*:* cpe:2.3:a:whatsapp:whatsapp:*:*:*:*:*:*:macos:*:* cpe:2.3:a:whatsapp:whatsapp_business:*:*:*:*:*:*:iphone_os:*:*	CWE-863
CVE-2025-43300	macOS: All versions before macOS Sequoia 15.6.1, macOS Sonoma 14.7.8, and macOS Ventura 13.7.8. iOS and iPadOS: All versions before iOS/iPadOS 18.6.2 and 17.7.10.	cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:*:* cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*:*	CWE-787

Recommendations

Update Immediately: Make sure you're running the latest version of WhatsApp on iOS or macOS. Both WhatsApp and Apple have patched the flaws, so updating the app and your operating system is the most important step you can take.

Restart Fresh if Alerted: If you received a threat notification from WhatsApp, follow their advice and perform a full factory reset of your device. This ensures any hidden traces of the attack are wiped out.

Turn On Auto-Updates: To stay ahead of future threats, enable automatic updates for both WhatsApp and your device's operating system so critical patches are installed without delay.

Be Cautious with Links: Since this attack involved malicious content loaded from URLs, avoid clicking on unexpected or suspicious links, even if they appear to come from someone you know.

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0002 Execution	T1203 Exploitation for Client Execution	T1204 User Execution
T1204.001 Malicious Link	T1588 Obtain Capabilities	T1588.006 Vulnerabilities	

Patch Details

Install the latest version of WhatsApp to address the flaw CVE-2025-55177.

Link:
https://www.whatsapp.com/download

For CVE-2025-43300, install the latest operating system versions:
iOS 18.6.2
iPadOS 18.6.2/17.7.10
macOS Sequoia 15.6.1, Sonoma 14.7.8, Ventura 13.7.8

Links:
https://support.apple.com/en-us/124925
https://support.apple.com/en-us/124926
https://support.apple.com/en-us/124927
https://support.apple.com/en-us/124928
https://support.apple.com/en-us/124929

References

https://www.whatsapp.com/security/advisories/2025/

https://x.com/DonnchaC/status/1961444710620303653

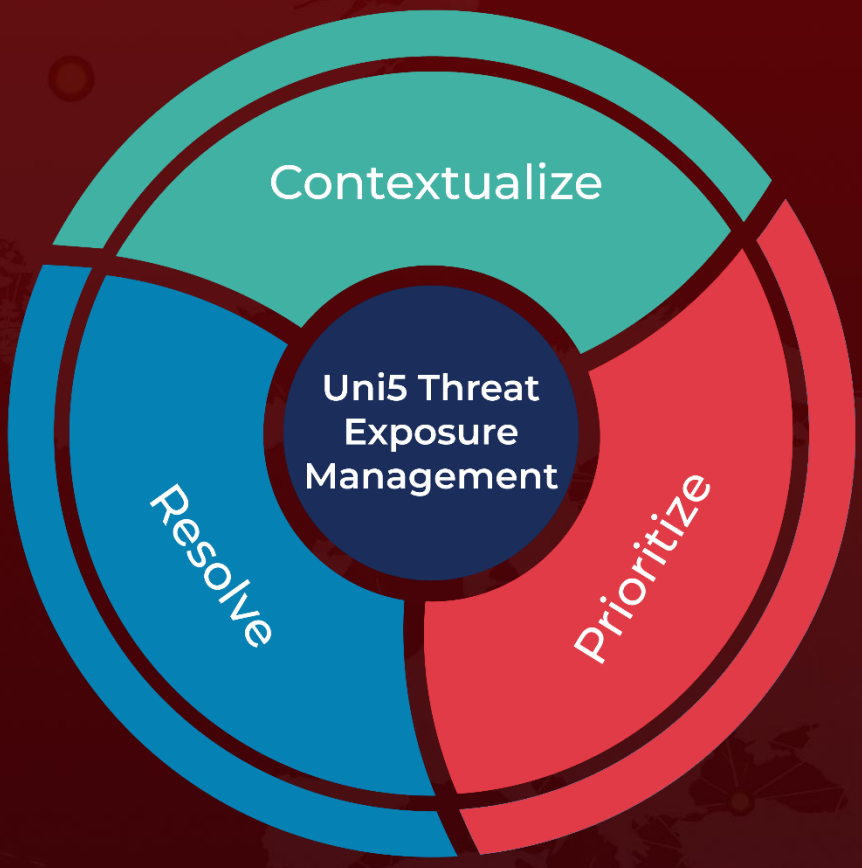
https://socradar.io/cve-2025-55177-0-click-whatsapp-exploit-spyware-apple/

http://hivepro.com/threat-advisory/cve-2025-43300-zero-day-in-apple-image-i-o-exploited-in-targeted-attacks/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

September 4, 2025 . 6:15 AM

More at www.hivepro.com