U UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0333

APPLE FIXES ZERO-DAY VULNERABILITIES

DATE ISSUED: 28th June 2023

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	[✓ MEDIUM]	EASY

OVERVIEW

Security researchers have discovered zero-day vulnerabilities in Apple, which are actively exploited in attacks. They can allow an unauthorised user to execute arbitrary code. They are leveraged to deliver triangulation spyware on iPhones via iMessage zero-click exploits.

BREAKDOWN

Kaspersky, a digital security firm, revealed details about a cyberattack that infects iPhones with spyware named "Operation Triangulation" by the company. Hackers could infect the iPhones using an “invisible iMessage with a malicious attachment” that can be activated without user interaction. The attack sequence starts when an iOS device receives an iMessage containing an attachment that carries the exploit. This exploit is described as zero-click, indicating that the vulnerability is triggered upon receiving the message without any user interaction necessary for executing the malicious code. The three zero-day vulnerabilities in Apple tracked as CVE-2023-32434, CVE-2023-32439 and CVE-2023-32435 are leveraged to deliver the Triangulation spyware on iPhones. They affect a wide range of Apple products ranging from iOS before 16.5.1, iPadOS before, 16.5.1mac OS Monterey before 12.6.7, macOS Big Sur before, 11.7.8 watchOS before 9.5.2, and macOS Ventura before 13.4.1.

REMEDIATION STEPS

- Apply the necessary updates provided by Apple.
- Implement an automated patch management solution to regularly perform operating system and application updates on enterprise assets.
- Update all credentials related to the affected appliances.
- Practice the Principle of Least Privilege on all systems and services to lower the risk of attacks.

REFERENCES & RESOURCES

Apple	https://support.apple.com/en-us/HT201222
Bleeping Computer	https://www.bleepingcomputer.com/news/apple/apple-fixes-zero-days-used-to-deploy-triangulation-spyware-via-imessage/
CIS Advisories	https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-apple-products-could-allow-for-arbitrary-code-execution_2023-066