Kaspersky exposed iPhone vulnerability at heart of Operation Triangulation

Kaspersky's Global Research and Analysis Team (GReAT) used the 37th Chaos Communication Congress in Hamburg to disclose a novel hardware feature within Apple iPhones that was instrumental in the Operation Triangulation campaign. The discovery, made public in late December 2023, highlights a vulnerability in the Apple System-on-a-Chip (SoC) which has been a pivotal factor in the recent spate of iPhone attacks.

Source: Markus Spiske/Unsplash

This vulnerability, identified in iPhones running up to iOS 16.6, allowed attackers to circumvent the hardware-based memory protection systems. It is believed that the hardware feature, which may have been originally designed for internal testing or debugging purposes, was exploited following an initial zero-click iMessage attack.

The exploitation enabled the attackers to bypass the device's security measures and alter the contents of protected memory areas, a critical step in gaining complete control over the iPhones. Apple has since responded to this security breach, designating it as CVE-2023-38606.

Cybersecurity threat trends show increased vulnerability for Apple devices

1 Aug 2023

As far as Kaspersky is aware, this feature was not publicly documented, presenting a significant challenge in its detection and analysis using conventional security methods. GReAT researchers engaged in extensive reverse engineering, meticulously analysing the iPhone's hardware and software integration, particularly focusing on the Memory-Mapped I/O, or MMIO, addresses, which are critical for facilitating efficient communication between the CPU and peripheral devices in the system.

Bypass hardware memory protection

Unknown MMIO addresses, used by the attackers to bypass the hardware-based kernel memory protection, were not identified in any device tree ranges, presenting a significant challenge. The team had to also decipher the intricate

workings of the SoC and its interaction with the iOS operating system, especially regarding memory management and protection mechanisms.

This process involved a thorough examination of various device tree files, source codes, kernel images, and firmware, in a quest to find any reference to these MMIO addresses.

“This is no ordinary vulnerability. Due to the closed nature of the iOS ecosystem, the discovery process was both challenging and time-consuming, requiring a comprehensive understanding of both hardware and software architectures," explained Boris Larin, principal security researcher at GReAT.

"What this discovery teaches us once again is that even advanced hardware-based protections can be rendered ineffective in the face of a sophisticated attacker, particularly when there are hardware features allowing to bypass these protections,”

> *“Operation Triangulation is an Advanced Persistent Threat (APT) campaign targeting iOS devices, uncovered by Kaspersky in 2023.”*

This sophisticated campaign employs zero-click exploits distributed via iMessage, enabling attackers to gain complete control over the targeted device and access user data. Apple responded by releasing security updates to address four zero-day vulnerabilities identified by Kaspersky researchers: CVE-2023-32434, CVE-2023-32435, CVE-2023-38606, and CVE-2023-41990.

These vulnerabilities impact a broad spectrum of Apple products, including iPhones, iPods, iPads, macOS devices, Apple TV, and Apple Watch. Kaspersky also informed Apple about the exploitation of the hardware feature, leading to its subsequent mitigation by the company.