iPhone Triangulation attack abused undocumented hardware feature

Originalartikel

Backup

<html> The Operation Triangulation spyware attacks targeting iPhone devices since 2019 leveraged undocumented features in Apple chips to bypass hardware-based security protections. This finding comes from Kaspersky analysts who have been reverse-engineering the complex attack chain over the past year, trying to unearth all details that underpin the campaign they originally discovered in June 2023. The discovery and use of obscure hardware features likely reserved for debugging and factory testing to launch spyware attacks against iPhone users suggest that a sophisticated threat actor conducted the campaign. Moreover, it constitutes an excellent example of why reliance on security through obscurity and the secrecy of hardware design or hardware testing implementation is a false premise. <h2>Operation Triangulation</h2> Operation Triangulation is a spyware campaign targeting Apple iPhone devices using a series of four zero-day vulnerabilities. These vulnerabilities are chained together to create a zero-click exploit that allows attackers to elevate privileges and perform remote code execution. The four flaws that constitute the highly sophisticated exploit chain and which worked on all iOS versions up to iOS 16.2 are: CVE-2023-41990: A vulnerability in the ADJUST TrueType font instruction allowing remote code execution through a malicious iMessage attachment.
CVE-2023-32434: An integer overflow issue in XNU's memory mapping syscalls, granting attackers extensive read/write access to the device's physical memory.
CVE-2023-32435: Used in the Safari exploit to execute shellcode as part of the multi-stage attack.
CVE-2023-38606: A vulnerability using hardware MMIO registers to bypass the Page Protection Layer (PPL), overriding hardware-based security protections. The attacks start with a malicious iMessage attachment sent to the target, while the entire chain is zero-click, meaning it does not require interaction from the user, and doesn't generate any noticeable signs or traces. Kaspersky discovered the attack within its own network, and Russia's intelligence service (FSB) immediately accused Apple of providing the NSA with a backdoor against Russian government and embassy personnel. So far, the origin of the attacks remains unknown, and there has been no proof of these allegations. Apple fixed the then-recognized two zero-day flaws (CVE-2023-32434 and CVE-2023-32435) on June 21, 2023, with the release of iOS/iPadOS 16.5.1 and iOS/iPadOS 15.7.7. <figure class=„image c2“><figcaption>Operation Triangulation attack chain (Kaspersky)</figcaption></figure> <h2>Highly sophisticated

attacks</h2> Of the above flaws, CVE-2023-38606, which was addressed on July 24, 2023, with the release of iOS/iPadOS 16.6, is the most intriguing for Kaspersky's analysts. Exploiting the flaw allows an attacker to bypass hardware protection on Apple chips that prevent attackers from obtaining complete control over the device when they gain read and write access to the kernel memory, which was achieved using the separate CVE-2023-32434 flaw. In the deep-dive technical writeup, Kaspersky explains that CVE-2023-38606 targets unknown MMIO (memory-mapped I/O) registers in Apple A12-A16 Bionic processors, likely linked to the chip's GPU co-processor, which are not listed in the DeviceTree. <figure class=„image c2“><figcaption>MIMO ranges targeted in the Triangulation attacks
(Kaspersky)</figcaption></figure> Operation Triangulation uses these registers to manipulate hardware features and control direct memory access during the attack. „If we try to describe this feature and how the attackers took advantage of it, it all comes down to this: they are able to write data to a certain physical address while bypassing the hardware-based memory protection by writing the data, destination address, and data hash to unknown hardware registers of the chip unused by the firmware,“ explains Kaspersky's report. Kaspersky hypothesizes that including this undocumented hardware feature on the finished consumer version of the iPhone is either a mistake or was left in to assist Apple engineers in debugging and testing. Apple fixed the flaw by updating the device tree to restrict physical address mapping. However, how the attackers gained knowledge of such an obscure exploitable mechanism in the first place remains unknown. </html>