January 5, 2024

Overall Rating - High

BRITISH COLUMBIA

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that new news events on existing Apple published security updates to address vulnerabilities in the following products:

- iOS and iPadOS – multiple versions
- macOS Big Sur – versions prior to 11.7.9
- macOS Monterey – versions prior to 12.6.8
- macOS Ventura – versions prior to 13.5
- tvOS – versions prior to 16.6
- watchOS – versions prior to 9.6

Technical Details

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.

These vulnerabilities are rated as an overall **High** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify VRM with any questions or concerns you may have.

References

- CVE-2023-41990, CVE-2023-32434, CVE-2023-32435, CVE-2023-38606
- https://support.apple.com/en-us/HT201222
- iPhone Triangulation attack abused undocumented hardware feature (bleepingcomputer.com)