Industry Security Alert

Critical Zero-Touch, Zero-Day RCE Vulnerability in Apple iOS/iPadOS 13.4.1

Introduction

Researchers at ZecOps [1] recently shared details of two vulnerabilities in Apple iOS that have reportedly been observed in targeted attacks against high-profile individuals, likely orchestrated by a nation-state threat actor. Exploiting these vulnerabilities requires specially crafted emails to be sent to a victim that consume large amounts of memory when processed by the default Apple Mail client and subsequently allow remote code execution (RCE) capabilities.

These vulnerabilities, whilst only detected as far back as January 2018, have existed since iOS 6 (publicly released on 19 September 2012 and shipped with the iPhone 5) and can be exploited on current Apple devices running iOS versions up-to and including the most recent iOS 13.4.1.

Given that the Apple iPad is also reported as affected by these vulnerabilities alongside the Apple iPhone, users should assume that Apple iPadOS versions up-to and including iPadOS 13.4.1 are also vulnerable. Prior to the release of iPadOS 3.1 (24 September 2019) both iPad and iPhone devices shared the same vulnerable releases of iOS.

Notably, malicious emails sent to a victim using iOS 13 do not require any user interaction to trigger the exploit as the exploit will be take place in the background.

Conversely, victims using iOS 12 are typically exploited if, and when, they click on the malicious email albeit prior to rendering any message content. It is reportedly possible for iOS 12 victims to be exploited without any interaction on their part if the threat actor has control over the mail server used to receive the malicious message.

Once exploited, it is likely that a threat actor would deploy other malicious code to gain control of a victim's device, allowing them to remove evidence of the compromise as well as stealing personal data and potentially conducting surveillance operations.

As of 15 April 2020, Apple have released beta versions of both iOS 13.4.5 and iPadOS 13.4.5 to developers, including patches to these vulnerabilities, that are likely to be made publicly available imminently. Details of an update for iOS 12 remains scarce, iOS 12.4.6 was the last public release (24 March 2020), and users of devices running older iOS versions, 6 through 11, will likely need to upgrade their device or implement a workaround to protect themselves from these critical vulnerabilities.

As is often the case in nation-state threat actors conducting operations against mobile devices, typically for espionage or surveillance purposes, reported targets have included business executives,

journalists and VIPs. Additionally, managed security service providers (MSSP) are also suggested targets, potentially to gain access to their customer's networks.

Vulnerability

Whilst ZecOps provide full technical detail of the exploits, both rely on the threat actor sending a specially crafted malicious email to the victim. Assuming the malicious email is processed by the Apple Mail application, in the context of the 'maild' process on iOS 13 or 'MobileMail' on iOS 12, it consumes large amounts of memory allowing two vulnerabilities to be exploited:

- An out-of-bounds (OOB) write vulnerability in the way that the MIME library lacks error checking and allows data to be written outside the bounds of allocated memory.
- A remote heap-overflow flaw, by not handling system call return values correctly, allowing data to overwrite allocated memory.

The exploit would be hard to detect by a victim using iOS 13, other than a temporary slowdown of the Apple Mail app, especially if the threat actor took steps to cover their tracks, whilst iOS 12 victims may only notice the Apple Mail app crashing (although many may not consider the relevance of this).

To avoid suspicion in the event of the exploits not being successfully triggered, or presumably if a victim finds the malicious email, the message body contains text such as "*This message has no content*" or "*The message cannot be displayed*".

Recommendations

In the first instance, most users with Apple iOS/iPadOS 13 devices should ensure that they install the iOS/iPadOS 13.4.5 update as soon as it is released.

Those that consider the threat to be sufficiently high, for example executives and VIPs, may wish to consider using an alternative email application and disabling the Apple Mail app on their mobile/tablet device, or, having taken into account the risks of using pre-release software, consider obtaining and deploying the iOS/iPadOS 13.4.5 beta update (available through the Apple Beta Software Program [2]).

Users of Apple devices running older versions of iOS may wish to consider either updating/upgrading to a device/iOS version that is currently supported by Apple and/or disabling the Apple Mail application and using an alternative.

[1] https://blog.zecops.com/vulnerabilities/unassisted-ios-attacks-via-mobilemail-maild-in-the-wild/

[2] https://beta.apple.com/sp/betaprogram/