iOS Mail Exploit

Overview

Recently, news broke of attacks exploiting two iOS vulnerabilities, which have existed since at least 2012. Both vulnerabilities affect the iOS MIME library and can be exploited via emails received by the iOS Mail app. The first vulnerability is an out-of-bounds write caused by a failure to correctly handle an error condition while the second vuln is a heap buffer overflow.

The attacks exploiting these vulnerabilities appear to have been used to target particular high-value individuals and corporations around the world, likely with the goal of surveillance / spying, but have not yet been attributed to a particular group of malicious actors.

How Does it Work?

The primary exploit involves a specially crafted email message sent to the target's email address. On iOS 12, the target has to open the email to activate the exploit chain. However, on iOS 13, the target never even has to open the message and it can be executed with zero touch as soon as the message is downloaded to the device by maild.

In both scenarios, the victim wouldn't notice any abnormal behavior aside from the Mail app crashing or some emails missing, as the attackers seem to delete the original email as part of their cover-up tactics. In isolation, these exploits do not give the attacker control over the target device - another exploit targeting a kernel vulnerability is needed to allow the attacker to gain privileged access.

Lookout Recommendation for Admins

At the point of publication, the initial vulnerability in Mail has only been patched in the beta release of iOS 13.4.5 and has not yet been distributed in the general software update. In order to be protected from this exploit, users should not be logged into the native Apple Mail app on their iOS devices and leverage other platforms for email.

In order to install spyware/surveillanceware, the attacker needs to accomplish a device compromise. Lookout's advanced device compromise detection will detect and alert on the device itself as well as in the MES console.

Lookout Threat Advisory Service

In the fast-changing world of mobile security, keeping your finger on the pulse can be challenging. Lookout Threat Advisory taps into the massive dataset from Lookout's global sensor network of millions of devices, pairing it with insight from its top security researchers to give you actionable intelligence on the latest mobile threats and risks.

Click here to learn more about Lookout Threat Advisory