Lookout

THREAT GUIDANCE

Zero Day in iOS 15.6.1

Overview

Apple released a software update to iOS and iPadOS 15.6.1 to patch a zero-day kernel vulnerability identified as CVE-2022-32917. Apple is aware of a report mentioning its active exploitation in the wild. This vulnerability is capable of allowing a maliciously crafted application to execute arbitrary code with kernel privileges. This CVE could affect Apple iPhone, iPads, and iPod Touch models, which means that anyone using one of these devices should immediately update their device by going to Settings, General, then Software Update. Apple has fixed this vulnerability in both iOS 15.7 and iOS 16.

This is the eighth zero day vulnerability[1] that has been fixed by Apple at the Operating System level this year. The iOS 15.7 update also covers 10 other vulnerabilities of varying criticality - including two webkit vulnerabilities that can also be exploited remotely via a crafted web page and the three kernel vulnerabilities that vary from giving privileged access to disclosing kernel memory.

Lookout Coverage and Recommendation for Admins

Lookout provides multilayered protection for devices that are exploitable through multiple vectors and could be compromised. To ensure your devices aren't exposed through the vulnerabilities in iOS 15.6.1 and earlier, Lookout admins should set default *OS Out of Date* policy to have a minimum iOS version of 15.7 for applicable models. They can then choose whether to alert the user that the device is out of compliance or block access to enterprise resources until iOS is updated.

In addition to requiring a minimum OS, admins should enable Lookout Phishing & Content Protection (PCP) to protect mobile users from malicious phishing campaigns that are built to exploit these vulnerabilities in order to phish credentials or deliver malicious apps

Lookout Analysis

Together, these CVEs could grant a remote user a control over the device by leveraging techniques such as Exploitation for Privilege Escalation (T1404), and Drive-by compromise (T1456) found in the MITRE mobile ATT&CK matrix. With reports of the kernel vulnerability under CVE-2022-32917 being actively exploited in the wild, we strongly suggest that the admins set policies that encourage their users to update their Apple devices to at least version 15.7. CVE-2022-32917 has been reported under CISA guidelines making it mandatory for all government agencies to follow the vendor guidelines of the security update.

Lookout Vulnerability and Patch Management

Lookout Vulnerability and Patch Management enables you to know every version of an operating system and mobile app in your organization. We provide visibility into device risk whether it is company- or employee-owned, as well as managed or unmanaged.

Click here to learn more about Vulnerability & Patch Management

[1] Other zero-day vulnerabilities fixed this year were: CVE-2022-22587, CVE-2022-22594, CVE-2022-22620, CVE-2022-22674, CVE-2022-22675, CVE-2022-32893, CVE-2022-32894