iOS 15.7.5/ iOS 16.4

Overview

Apple recently released two critical updates for iOS with heavy security implications. iOS 16.5 and iOS 15.7.6 patch a combined 56 issues, which include 3 critical webkit vulnerabilities. Not only are these actively exploited zero-day vulnerabilities, but they also made it to the CISA list of mandatory fixes for the government organizations.

Two of these critical webkit vulnerabilities were included in the latest Rapid Security Response (RSR), which is Apple's new system of delivering security patches to devices running the latest version of iOS. It is important to note that all the fixes of the RSR released on May 01,2023 have been rolled into the latest OS releases. Apple did not disclose the security content of the RSR until the latest OS release. In order to ensure protection, users should update all Apple devices to the latest OS version.

Lookout Coverage and Recommendation for Admins

To ensure your devices aren't exposed through the vulnerabilities in iOS 15.7.5 and earlier or upto 16.4 in iOS 16 series, Lookout admins should set default *OS Out of Date* policy to have a minimum iOS version of 16.5 for applicable models.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 to the device. Finally, Lookout will detect if an attacker is successfully able to compromise the device at the OS level.

Lookout Analysis

Since these vulnerabilities are actively exploitable, remotely executable, and mentioned by CISA as required patches for government organizations, it is critical that every organization ensure its devices are up to date. The three critical webkit-related CVEs are:

1. CVE-2023-32409 : A remote attacker may be able to break out of Web Content sandbox
2. CVE-2023-28204 : Processing web content may disclose sensitive information
3. CVE-2023-32373 : Processing maliciously crafted web content may lead to arbitrary code execution

It should be noted that CVE-2023-28204 and CVE-2023-32373 were fixed in patch 16.4.1(a) — an RSR released in May. For enterprise organizations, it's always good to follow suit when CISA finds something critical enough that government organizations should patch it. As has been observed in the past, cyber attacks that target government often target businesses further down the line.

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