iOS WebKit Vulnerabilities

Overview

Apple released urgent software updates to both iOS 14.4 and 14.5 to patch serious vulnerabilities in Apple's WebKit browser engine. In each case, the vulnerabilities were actively being exploited in the wild according to Apple. These urgent security patches are not the first ones that that Apple released for iOS 14, as there were three highly critical vulnerabilities found in iOS 14.3 earlier in 2021. Apple has deemed these vulnerabilities serious enough to release an update for devices that can only run up to iOS 12, such as iPhone 5s, 6, and older iPads.

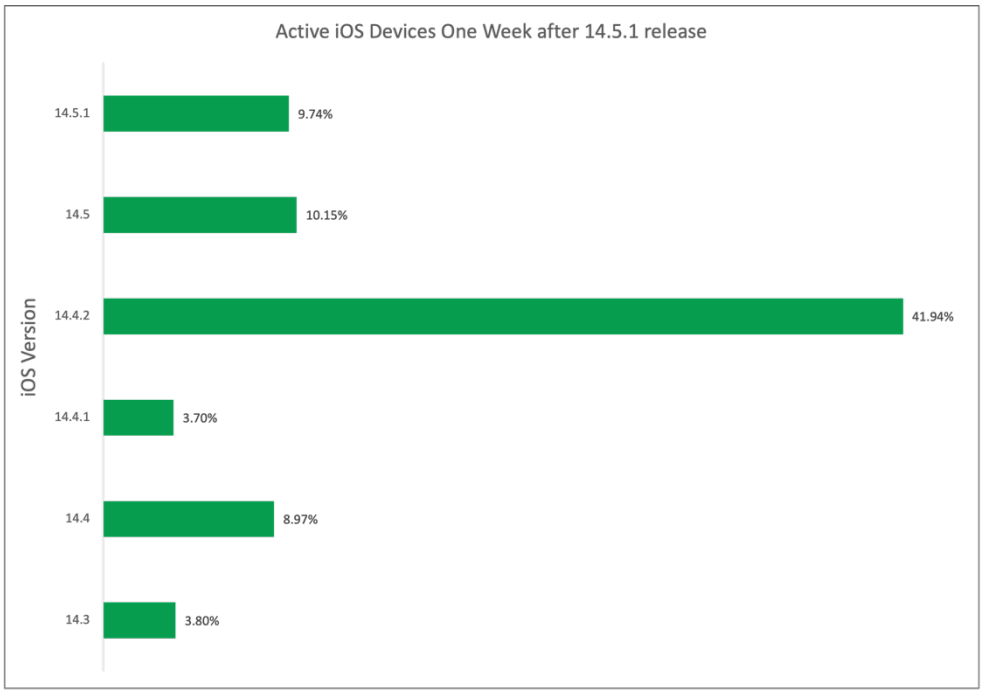
Lookout Coverage and Recommendation for Admins

With Vulnerability and Patch Management, Lookout admins can set the default OS Out-of-Date policy to have a minimum compliant iOS version of 14.5.1 From there, admins can choose whether to simply alert the user that the device is out of compliance or completely block access to corporate resources until iOS is updated.

In addition, Lookout Phishing & Content Protection will help protect mobile users from malicious phishing campaigns built to exploit these vulnerabilities. Lookout PhishingAI constantly monitors the web for new sites built specifically for phishing purposes and implements protection against them in near real-time.

Lookout Analysis

While Apple hasn't released many details about these vulnerabilities, a successful exploit could allow malicious websites to perform arbitrary cross-scripting on the device. This means that an attacker could easily redirect the victim to a malicious page they built, phish login credentials for personal or corporate accounts, or deliver malware to the device to spy on the user or exfiltrate files from any cloud-based service that user has access to. In addition, the attacker could perform actions on the user's behalf on malicious sites.



Analysis of the Lookout Security Graph shows that a significant number of enterprise mobile devices are still on iOS 14.4.2. While this means they're not exposed to the first round of WebKit vulnerabilities, they are still exposed to the vulnerabilities patched in 14.5.1.

Since this vulnerability exists in WebKit, it could also be used inside iOS apps. This incident exemplifies why attackers have found that delivering phishing links through platforms like social media, third-party messaging apps, gaming, and even dating apps makes it easier to socially engineer mobile users.

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 independent of whether it is company- or employee-owned, as well as managed or unmanaged.

Click here to learn more about Vulnerability & Patch Management