iOS 14.3 Vulnerabilities

Overview

Apple notified iPhone users of three major vulnerabilities in iOS 14.3 that are actively being exploited in the wild. CVE-2021-1872, which appears to be the most critical, exploits a flaw in the iOS kernel that could allow malicious apps to elevate privileges on the device. The other two CVEs, 2021-1870 and 2021-1871, exploit flaws in Apple's WebKit engine for Safari and could allow an attacker to execute malicious code remotely. Researchers suspect that attackers combine these vulnerabilities to gain full control of iOS devices remotely.

Lookout Analysis

Considering the nature of these vulnerabilities, an attacker could easily build a malicious app and distribute it via social engineering across social media platforms, SMS messages, third-party chat apps, and even dating or gaming apps. With the same strategy, they could build mobile-specific phishing campaigns that are delivered in a similar fashion and exploit the WebKit vulnerability.

This group of vulnerabilities illustrates the importance of always updating your mobile device's operating system. Regardless of the device or operating system it runs on, updates are almost always centered around security patches. For the sake of keeping both personal and corporate data secure, a serious vulnerability in the kernel of the device should be patched without hesitation. In the case that your organization embraces BYOD, it's even more critical that all users update their devices as attackers will leverage personal apps that deliver malicious payloads to out-of-date iPhones.

Lookout Coverage and Recommendation for Admins

With Mobile Vulnerability and Patch Management, Lookout admins can set the default OS Out-of-Date policy to have a minimum compliant iOS version of 14.4. 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 Mobile Vulnerability and Patch Management

Lookout Mobile 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 Mobile Vulnerability & Patch Management