iOS 15.3

Overview

Apple released an urgent software update to iOS 15.3 to patch a serious vulnerability in Apple's WebKit browser engine. This vulnerability could enable attackers to execute arbitrary code remotely on the device. Exploiting this vulnerability can be most closely associated with a universal cross-site scripting (UXSS) attack, which can exploit client-side vulnerabilities in the browser or its extensions to affect the behavior of the browser itself. An arbitrary code execution would enable the attacker to bypass or disable any default security features the browser may have. This tactic can be used to deliver malware to a device, siphon or phish for login credentials on most websites, and even be an entry point for attackers to completely compromise the device.

Lookout Coverage and Recommendation for Admins

Lookout provides multilayered protection for devices that are exploitable through multiple vectors and could be compromised. The best way to ensure your devices aren't exposed through the vulnerabilities in iOS 15.3 and earlier, Lookout admins should set default *OS Out of Date* policy to have a minimum iOS version of 15.3.1. 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

Analysis of the Lookout Security Graph shows that the majority of enterprise iOS devices are still on iOS 15.2.1 or earlier. This means these devices are exploitable via the WebKit vulnerabilities in 15.3 and could be leaking browsing history data as part of a Safari vulnerability from 15.2.1.

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

Click here to learn more about Vulnerability & Patch Management