iOS 15.0.1

Overview

In response to the latest zero-day vulnerability discovered in a new version of iOS, Apple released an urgent software update for iOS 15.0.1 to patch a serious vulnerability in the IOMobileFrameBuffer. This vulnerability was noted to be knowingly exploited in the wild and could allow an application to execute code with kernel privileges. This would also put the device in a compromised state. There has also been research that suggests this vulnerability is exploitable through the mobile browser, which is particularly concerning as it gives threat actors behind phishing campaigns a direct route into admin privileges on the targeted device.

Recommendation for Lookout Admins

Every Apple device user in your fleet should update their operating system to the latest version immediately and ensure the Phishing and Content Protection (PCP) is enabled. Lookout admins can enforce these two settings by setting a minimum OS policy for any device with Lookout for Work installed on it and requiring devices to have PCP enabled. Users are alerted and protected if the device enters a compromised state with one of the default policies in the Lookout admin console.

To enforce a minimum OS policy, you can go to Protections in the Lookout admin console, select the device policy ‘OS Out-Of-Date’, and select iOS 14.8 as the minimum compliant version. From there, the admin can choose whether to alert the device or, to ensure the update is carried out, block the device’s access to company resources until it’s compliant.

To protect your users from phishing links in any mobile app, require PCP on every device by going to Protections in the Lookout admin console, selecting “Phishing and Content Protection” at the top, and toggling the “Make Phishing and Content Protection mandatory” option.

Lookout Analysis

On mobile devices, socially engineered phishing links can be sent through SMS, email, social media platforms, third party messaging apps, gaming and even dating apps. Regardless of whether your organization allows employees to use personal devices in a BYOD model, requires devices to have mobile device management (MDM), or issues corporate devices, attackers will always be able to leverage at least a couple of these channels to deliver phishing links to users.

Regardless of how the exploit is delivered, it’s also important to note that a successful attack will put the device in a compromised state. Device-level vulnerability exploitations often do this in a discrete way, so the victim doesn’t know that their devices has been taken over. Detecting advanced device compromise can be the difference between keeping your organization safe and falling victim to a cyber attacker.

Lookout Threat Advisory Service

In the fast-changing world of mobile security, keeping your finger on the pulse can be challenging. Lookout Threat Advisory taps into the massive dataset from Lookout’s global sensor network of millions of devices, pairing it with insight from its top security researchers to give you actionable intelligence on the latest mobile threats and risks.

Click here to learn more about Lookout Threat Advisory