



iOS 14.8 Update



Overview

Apple released an urgent software update for iOS 14.7 to patch a serious vulnerability that was found to be exploitable by attackers using the advanced surveillanceware known as Pegasus. This vulnerability was discovered by The Citizen Lab while investigating an anonymous Saudi activist's phone and dubbed **FORCEDENTRY**. It targets Apple's graphics rendering library, which makes it effective against iOS, MacOS, and WatchOS devices. Discovery of **FORCEDENTRY** shows that the NSO Group continues to find new ways to exploit devices and enable its customers to spy on targeted individuals. According to The Citizen Lab, **FORCEDENTRY** has been in use since at least February 2021.

The vulnerability is noted to process maliciously crafted PDF files that may lead to arbitrary code execution on the target device. The Citizen Lab observed additional evidence, such as use of the **CASCADEFAIL** bug as well as the process names being exploited, that were used by NSO to deliver Pegasus in the past and helped them draw the conclusion that the observed device was targeted with the surveillanceware.

Recommendation for Lookout Admins

Every Apple device user in your fleet should update their operating system to the latest version immediately. Lookout admins can enforce this by setting a minimum OS policy for any device with Lookout for Work installed on it. To do this, you can go to Protections in the Lookout admin console, select the device policy 'OS Out-Of-Date', and select iOS 14.8 as the minimum compliant version.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.

Lookout Analysis

This is the latest in a consistent stream of news surrounding Pegasus and the NSO Group. Since Lookout and The Citizen Lab discovered Pegasus in 2016, it has continued to evolve and become more advanced. Most notably, NSO prioritizes use of the zero-click exploit in recent iterations of Pegasus, as was observed in an earlier vulnerability in the VOIP functionality of WhatsApp in 2019 as well as one in iMessage in 2020. Zero-click delivery means that the operator can send a malicious link or file to the device and the surveillanceware will infect the device without the target even knowing.

Mobile devices continue to be a primary attack vector for cyber criminals. Mobile malware, surveillanceware, and ransomware can take down infrastructure and track our every move as attackers target individuals where they are most vulnerable. Business executives with access to market data, technological research, and infrastructure are highly valuable targets. As iOS and Android devices continue to be integral to our lives, they need to be secured with as much, if not more priority than any other device.

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](#)