



iOS 16.3



Overview

Apple recently released iOS 16.3.1, which includes a number of <u>critical security fixes</u> for vulnerabilities including CVE-2023-23514 and CVE-2023-23529, which is the latest zero day vulnerability to affect Apple devices. Apple is aware of this zero day being potentially exploited, which makes it particularly important to patch any affected devices as soon as 16.3.1 is available. CISA is currently mandating government organizations to update to iOS 16.3.1 by March 7th, 2023.

16.3.1 is available for iPhone 8 and later, iPad Pro and iPad Air 3rd generation and later, iPad 5th generation and later, and iPad mini 5th generation and later. Anyone using one of these devices should immediately update their device.

Lookout Coverage and Recommendation for Admins

Lookout provides multilayered protection for devices that are exploitable through multiple vectors. To ensure your devices aren't exposed through the vulnerabilities in iOS 16.3 and earlier, Lookout admins should set default *OS Out of Date* policy to have a minimum iOS version of 16.3.1 for applicable models. 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 could exploit these vulnerabilities to phish credentials or deliver malicious apps to the device.

CISA mandates all government organizations to update to the patched versions of CVE-2023-23529 (16.3.1) by March 7th, 2023.

Lookout Analysis

CVE-2023-23514 enables an attacker to execute arbitrary code with kernel privileges while CVE-2023-23529 allows maliciously crafted web content to arbitrarily execute code and could also grant privileges. Exploit reports of CVE-2023-23529 were known before the patch was released. Together, these CVEs could grant an attacker a dangerous amount of control by leveraging techniques such as T1404 (Exploitation for Privilege Escalation) and T1456 (Drive-By Compromise) in the MITRE mobile ATT&CK matrix.

Since this chain can be executed remotely, it is important to patch the devices as soon as possible. It has also been listed under CISA guidelines making it mandatory for all the government agencies to implement the update. For enterprise organizations, it's always good to follow suit when CISA finds something critical enough that government organizations should patch it. As has been observed in the past, cyber attacks that first target the government are often found targeting businesses further down the line.

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