





### Overview

iOS 16.4.1 includes two critical fixes for two zero day vulnerabilities, CVE-2023-28206 and CVE-2023-28205, that have known exploits in the wild. CISA is currently mandating government organizations to update to iOS 16.4.1 by May 1st, 2023. Just over a week after the release of 16.4, these fixes were released over the weekend to ensure timely reach to the devices.16.4.1 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your devices aren't exposed through the vulnerabilities in iOS 16.4 and earlier, Lookout admins should set default *OS Out of Date* policy to have a minimum iOS version of 16.4.1 for applicable models.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, 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-2023-28206 and CVE-2023-28205 (16.4.1) by May 1st, 2023.

# Lookout Analysis

CVE-2023-28206 (issue in IOSurfaceAccelerator) enables an attacker to use maliciously crafted applications to execute arbitrary code with kernel privileges on targeted devices. CVE-2023-28205 (a WebKit flaw) allows maliciously crafted web content to arbitrarily execute code granting privileges. Reports of exploits for both CVEs 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

© 2023 Lookout, Inc. LOOKOUT®, the Lookout Shield Design®, LOOKOUT with Shield Design®, and SIGNAL FLARE® are registered trademarks of Lookout, Inc. in the United States and other countries. DAY OF SHECURITY®, LOOKOUT MOBILE SECURITY®, and POWERED BY LOOKOUT® are registered trademarks of Lookout, Inc. in the United States. Lookout, Inc. maintains common law trademark rights in EVERYTHING IS OK, PROTECTED BY LOOKOUT, CIPHERCLOUD, SCREAM, the 4 Bar Shield Design, and the Lookout multi-color/multi-shaded Wingspan design.