



iOS 16.1.1 and 16.1.2



Overview

Apple recently released two software updates with security fixes: iOS 16.1.2 and iOS 16.2. While users can update to 16.2 to patch the vulnerabilities covered in both updates, CISA is mandating government organizations to update to 16.1.2 by January 4th, 2023 to patch iOS 16.1.1 and lower, which has been found to have an exploitable zero day vulnerability.

The update to version 16.1.2 has a security fix for CVE-2022-42856, which is being actively exploited according to Google's Threat Analysis Group. It can be exploited remotely via a maliciously crafted webpage and enables the attacker to arbitrarily execute code on the affected device. It's important to note that older models that cannot upgrade to iOS 16 can be patched by updating to 15.7.2.

The iOS 16.2 update includes a list of 35 security fixes against the following vulnerabilities and possible exploits:

- Allows kernel code execution: CVE-2022-46694, CVE-2022-42848, CVE-2022-42850, CVE-2022-42846, CVE-2022-46690, CVE-2022-42837, CVE-2022-46689, CVE-2022-42845, CVE-2022-42840
- 2. Capable of remote code execution potentially granting privileged access: CVE-2022-46693, CVE-2022-42864, CVE-2022-42842, CVE-2022-42867, CVE-2022-46691, CVE-2022-42852, CVE-2022-46696, CVE-2022-46699, CVE-2022-46700, CVE-2022-42863
- 3. Compromising privacy or personal information disclosure: CVE-2022-42851, CVE-2022-42862, CVE-2022-46698,

Both OS updates are 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devices aren't exposed through the vulnerabilities in iOS 16.1.2 and earlier, Lookout admins should set default *OS Out of Date* policy to have a minimum iOS version of 16.2 for applicable models.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.

We highly recommend nudging users to the latest available OS that their device can handle. CISA mandates all government organizations to update to the patched versions of CVE-2022-42856 (16.1.2/15.7.2) by January 4th, 2023.

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