



iOS 16 Zero Day



Overview

Apple recently released a software update to iOS 16.1 and iPadOS 16 to patch a zero-day kernel vulnerability identified as CVE-2022-42827, which is reportedly being exploited in the wild. This vulnerability could allow a maliciously crafted application to execute arbitrary code with kernel privileges. The patch 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 by going to Settings, General, then Software Update.

Some of the notable vulnerabilities of the 19 patched in this update include:

- CVE-2022-32947, CVE-2022-32940, CVE-2022-32924, CVE-2022-42808, CVE-2022-42827, CVE-2022-42829 - 32, CVE-2022-32922 which are capable of remote code executions that grant privileged access to disclosing kernel memory.
- CVE-2022-42811 and CVE-2022-42824, which could disclose sensitive information via malcrafted webpages.
- CVE-2022-32946 which represents a flaw in the Bluetooth component, which can allow an app to record audio using AirPods

Lookout Coverage and Recommendation for Admins

Lookout provides multilayered protection for devices that are vulnerable through multiple vectors. Lookout admins should set default *OS Out of Date* policy to have a minimum iOS version of 16.1 for applicable models.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 exploit these vulnerabilities to phish credentials or deliver malicious apps to the device.

CISA is requiring all government organizations to update to the patched versions of these apps by November 15th.

Lookout Analysis

These CVEs could grant a remote user a control over the device by leveraging techniques such as *exploitation for privilege escalation* (T1404) and *drive-by compromise* (T1456) found in the MITRE mobile ATT&CK matrix. We strongly suggest that the admins set policies that encourage their users to update their Apple devices to at least version iOS 16.1 and iPadOS 16.0. CVE-2022-42827 has been reported under CISA guidelines making it mandatory for all government agencies to run the security update.

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](#)