



iOS 15.5 Vulnerabilities



Overview

Apple released a software update to iOS and iPadOS 15.5 to patch over 35 issues that had potential effects ranging from remote code execution to UI spoofing and user activity tracking. Almost every security issue in 15.5 could affect Apple iPhone, iPads, and iPod Touch models that have been available for years, which means that anyone using one of these devices should immediately update their device by going to Settings, General, then Software Update.

Lookout Coverage and Recommendation for Admins

Lookout provides multilayered protection for devices that are exploitable through multiple vectors and could be compromised. To ensure your devices aren't exposed through the vulnerabilities in iOS 15.5 and earlier, Lookout admins should set default *OS Out of Date* policy to have a minimum iOS version of 15.6 for applicable models.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.

Admin should also enable Lookout Phishing & Content Protection (PCP) to protect mobile users from malicious phishing campaigns that are built to exploit these vulnerabilities in order to phish credentials or deliver malicious apps to the device. Finally, Lookout will detect if an attacker is successfully able to compromise the device at the OS level.

Lookout Analysis

Within the long list of security issues, Lookout has identified two particularly critical vulnerabilities that can grant malicious actors control over the device from anywhere. The first, CVE-2022-32788 is a buffer overflow vulnerability that a remote user could exploit to execute code remotely in the kernel of the device. The other vulnerability, identified as CVE-2022-32839, could enable a remote user to execute arbitrary code or cause an unexpected app termination. Additional details of the CVE have not been released yet for security reasons.

Together, these CVEs could grant a remote user a dangerous amount of control over the device by leveraging techniques such as [T1437](#) & [T1428](#) found in the MITRE [mobile ATT&CK matrix](#). These techniques enable remote execution capabilities at an OS level and can obfuscate them under an application layer.

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](#)