iOS Vulnerabilities

Overview

Apple released a software update to iOS and iPadOS 15.6 to patch two core zero-day vulnerabilities, CVE-2022-32894 (Kernel) and CVE-2022-32893 (Webkit), which together form a full kill chain. The entry in the system could be via a crafted web content or an application and will allow a system takeover in the event of an active exploitation. There is evidence of active exploitation in the wild for these vulnerabilities already. Both of these CVEs 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.

This update comes hot on the heels of another recent iOS update at the end of July, which patched over 35 vulnerabilities in the mobile operating system. Much like the vulnerabilities in 15.6, they could enable remote execution capabilities at the OS level.

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your devices aren't exposed through the vulnerabilities in iOS 15.6 and earlier, Lookout admins should set default *OS Out of Date* policy to have a minimum iOS version of 15.6.1 for applicable models.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 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

Both of these vulnerabilities are being actively exploited in the wild. They have been reported under CISA guidelines making it mandatory for all the government agencies to follow the vendor guidelines of the security 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.

Together, these CVEs could grant a remote user a dangerous amount of control over the device by leveraging techniques such as T1404 (Exploitation for Privilege Escalation) and T1456 (Drive-By Compromise) found in the MITRE mobile ATT&CK matrix.

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