



8 iOS & Android CVEs



Overview

CISA recently announced several exploitable mobile vulnerabilities that can affect both Android and iOS devices. They vary in severity and can be deployed by leveraging a variety of exploitation mechanisms. The most concerning risk comes from those that do not require user interaction to be executed.

CVE-ID	Affected versions/ OS	Impact	Exploit mechanism	Lookout's Recommendation
CVE-2019-18426	WhatsApp Desktop versions < 0.3.9309 paired with WhatsApp for iPhone versions < 2.20.10	When the desktop version is paired with vulnerable mobile versions, it allows cross-site scripting and local file reading.	Exploitation requires the victim to click a link preview from a specially crafted text message.	WhatsApp on iPhone with a version 2.20.10 or later Lookout app coverage: <i>WhatsApp-CVE-2019-18426</i>
CVE-2019-5786	Google Chrome versions prior to 72.0.3626.121 Android only	Object lifetime issue in Blink	Allows remote attacker to potentially perform out of bounds memory access via a crafted HTML page	Version update Lookout app coverage: <i>Chrome-CVE-2019-5786</i>
CVE-2019-11707	Mozilla Firefox ESR < 60.7.1 and <67.0.3 Android only	A type confusion vulnerability that can occur when manipulating JavaScript objects due to issues in Array.pop	Allows an exploitable crash.	Fixed in Firefox for Android 67.0.3 Lookout app Coverage: <i>Firefox-CVE-2019-11707</i>

iOS

CVE-2019-7287	iOS 12.1.3 and below	A memory corruption vulnerability. It was addressed with improved input validation	An application may be able to execute arbitrary code with kernel privileges	Fixed in iOS 12.1.4
CVE-2019-7286	iOS 12.1.3 and below, macOS, watchOS, and tvOS	Memory corruption vulnerability	An application may be able to gain elevated privileges	Fixed in iOS 12.1.4
CVE-2021-30883	iOS 15.0.1 and below, macOS, watchOS, and tvOS	Contains a memory corruption vulnerability that could allow for remote code execution.	An application may be able to execute arbitrary code with kernel privileges.	Fixed in iOS 15.0.2
CVE-2016-4657	WebKit in Apple iOS before 9.3.5	It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption)	Can be exploited remotely via a crafted web site	Fixed in iOS 9.3.5
CVE-2016-4656	Apple iOS before 9.3.5	A memory corruption vulnerability in Apple iOS kernel	Can be exploited remotely via a crafted application.	Fixed in iOS 9.3.5

		allows attackers to execute code in a privileged context or cause a denial-of-service		
CVE-2016-4655	Apple iOS before 9.3.5	The kernel in iOS allows attackers to obtain sensitive information from memory	Can be exploited remotely via a crafted application.	Fixed in iOS 9.3.5

Android

CVE-2021-0920	Android	Android kernel contains a race condition, which allows for a use-after-free vulnerability.	User interaction is not needed for exploitation. Exploitation can allow for privilege escalation.	ASPL 2021-11-06 or later
CVE-2021-1048	Android	Android kernel contains a use-after-free vulnerability	This could lead to local escalation of privilege with no additional execution privileges needed.	ASPL 2021-11-06 or later

Coverage and Recommendation for Lookout Admins

Lookout admins should proactively enable the vulnerability protection policy in the Lookout console and configure it with the appropriate severity and remediation actions that align with their organization's response workflows. As of June 9th, 2022, Lookout will alert on Chrome for Android versions 72.0.3626.120 or before as well as Firefox for Android versions 67.0.2 or before as vulnerable.

Lookout Analysis

Successful exploitation of these vulnerabilities can only happen if the device user has not updated to the latest version of iOS or Android. Attackers try to take advantage of this gap between when a vulnerability is announced and when the user runs that update, which most end-users will not do immediately. A successful exploit may impact in the ways listed above without needing to root the device. Mobile device management (MDM) tools will not detect a successful exploitation. In the event of a successful exploit, the actor could gain privileged access.

Lookout Mobile Vulnerability and Patch Management

Lookout Mobile Vulnerability and Patch Management enables you to know every operating system and mobile app version in your fleet. We provide visibility into device risk whether it is company- or employee-owned, managed, or unmanaged. Lookout crowdsources the most comprehensive vulnerability and patch management database from analysis of nearly 205 million mobile devices and over 170 million apps. It correlates the app and operating system versions needed to patch vulnerabilities. In addition, the database specifies the version of the operating system that is specific to a carrier and device manufacturer for the patch.

[Click here to learn more about Lookout Mobile Vulnerability and Patch Management](#)