



# Chrome for Android



## Overview

Google recently discovered and disclosed an exploitable vulnerability in Chrome for Android, Windows, and Mac. The Android-specific vulnerability, which is identified as CVE-2020-16010, was reported by members of the Google Project Zero team.

According to the report, the vulnerability exists due to a heap-based buffer overflow that is triggered when Google Chrome on Android renders maliciously crafted HTML content. Successfully exploiting the vulnerability may allow the attacker to compromise the entire affected device.

## Lookout Analysis

Google has noted that there are already exploits for this vulnerability in the wild, which explains the rapid turnaround from reporting the vulnerability to releasing an app update. Based on telemetry from our Lookout Security Graph, which is informed by tens of millions Android users protected by Lookout Personal and Lookout for Work, we estimate that up to 50% of Android users globally are running an out of date version of Chrome for Android.

A successful exploit could allow the actor to perform a sandbox escape via a crafted HTML page, which means the actor can gain access to Chrome's capabilities 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 have access to any capability that the browser has. This includes access to the camera and microphone, location data, browsing history and more.

## Lookout Coverage and Recommendation for Admins

Lookout will detect any version of Chrome before 86.0.4240.185 as a vulnerable application in your fleet. Since Chrome is the primary browser on Android devices, admins should proactively enable the vulnerability protection in the Lookout console and configure it with the appropriate severity and remediation actions that align with their organization's response workflows.

## Lookout Mobile Vulnerability and Patch Management

Lookout Mobile 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 independent of whether it is company- or employee-owned, as well as managed or unmanaged. Lookout crowdsources the most comprehensive vulnerability and patch management database from analysis of nearly 200 million mobile devices and over 120 million apps. It correlates the app and operating system versions needed to patch vulnerabilities. In addition, the database specifies the version of 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](#)