



CVE-2022-1096



Overview

An anonymous researcher recently discovered and disclosed an exploitable vulnerability in Chromium, which is the codebase that provides the vast majority of code for the Google Chrome browser. The vulnerability, which is identified as CVE-2022-1096, was reported to exist in the *V8 Javascript Engine* component of Chromium and can be exploited with a malcrafted webpage. Successfully exploiting the vulnerability may allow the attacker to compromise the user's data on a vulnerable device.

Lookout Analysis

Google has noted that there are already exploits for this vulnerability in the wild on Chrome for desktop, which explains the rapid turnaround from reporting the vulnerability to releasing an app update. In addition to the known exploit that can affect desktop platforms, Lookout sees evidence that indicates that this vulnerability also affects the Android version of Chrome. Every user should update to the latest version of Chrome for Android, 99.0.4844.84, available on Google play for most devices. In addition, United States Federal entities should heed CISA's requirement to have it patched by April 18th, 2022.

The most likely way for an attacker to exploit this vulnerability would be to send a link leading to a malcrafted webpage to their target in hopes that the target still has a vulnerable version of Chrome on their device. A successful exploit may grant a threat actor 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.

Coverage and Recommendation for Lookout Admins

Since Chrome is one of the most widely-used browsers, 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. Starting April 7th, 2022, Lookout will alert on Chrome versions 99.0.4844.83 or before as vulnerable.

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. Lookout crowdsources the most comprehensive vulnerability and patch management database from analysis of nearly 200 million mobile devices and over 160 million apps.

[Click here to learn more about Vulnerability & Patch Management](#)