



CVE-2022-3075



Overview

Google recently released a patch for a new zero-day vulnerability found in the Chromium open-source web browser project, which provides the codebase behind popular web browsers including Google Chrome and Microsoft Edge. The vulnerability is tracked as CVE-2022-3075 and according to Google, exists due to “insufficient data validation” in the runtime libraries that Chromium is based on. Google has disclosed that the vulnerability is currently known to be actively exploited, making this disclosure a concern for any organization or individual that leverages the Chrome browser across Android, Windows, Mac, or Linux.

In addition to Chrome, Microsoft Edge also uses this component for its Android app - making it vulnerable to CVE-2022-3075. In response to the disclosure of this zero-day, Microsoft released a patch for their browser as well. This is the sixth zero-day vulnerability found in Chromium in 2022.

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 remediation actions that align with their organization’s response workflows. As of September 22nd, 2022, Lookout will alert on Chrome for Android versions 105.0.5195.123 or before and Edge for Android versions 105.0.1343.26 or before as vulnerable apps. In addition, CISA is requiring all government organizations to update to the patched versions of these apps by September 29th.

Lookout Analysis

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.

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 over 210 million mobile devices and 175 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](#)