CVE-2022-4135

Overview

Google recently released a patch for a new zero-day vulnerability, tracked as CVE-2022-4135, found in the Chromium open-source web browser project, which provides the codebase for many popular browsers. This vulnerability is reported to be of critical severity at a CVSS 3.x score of 9.6 and exists in the GPU component causing a heap buffer overflow. Reportedly, this CVE affects older versions of Google Chrome and Microsoft Edge, and patches have been released for both in response to this zero-day. 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.

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 December 8th, 2022, Lookout will alert on Chrome for Android versions 107.0.5304.140 or before and Edge for Android versions 107.0.1418.61 or before as vulnerable apps. In addition, CISA is requiring all government organizations to update to the patched versions of these apps by December 19th, 2022.

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. It can enable threat actors to crash a program or execute codes remotely. 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. Per NIST's national vulnerability database, this can arm "a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page"

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