CVE-2022-4262

Overview

Google recently released an emergency patch for a new zero-day vulnerability tracked as CVE-2022-4262. The CVE is found in the V8 Javascript engine of Chromium open-source web browser project, which provides the codebase for many popular browsers including Google Chrome and MS Edge. This vulnerability has been listed in the CISA's known exploited vulnerabilities catalog after Google disclosure of CVE-2022-4262's active exploitation in the wild, making this disclosure a concern for any organization or individual that leverages the Chromium based browsers (Chrome and Edge) across Android, Windows, Mac, or Linux.

Coverage and Recommendation for Lookout Admins

With new zero-day vulnerabilities being discovered and disclosed with increased frequency, Lookout strongly suggests all mobile device users turn on the app auto-update capability on their respective devices. 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 15th, 2022, Lookout will alert on Chrome for Android versions 108.0.5359.78 or before and MS Edge for mobile versions 108.0.1462.40 or below. In addition, CISA is requiring all government organizations to update to the patched versions of these apps by December 26th, 2022.

Lookout Analysis

The most likely way to exploit this vulnerability would be to send a link to a malcrafted webpage to a target in hopes that the target still has a vulnerable version of Chrome or Edge on their device. A successful exploit may grant a threat actor access to the browser's capabilities without needing to root the device and can also enable threat actors to crash a program or execute codes remotely. It should be noted that 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 to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)"

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