CVE-2022-1633 – 1641

Overview

External researchers recently discovered and disclosed to Google nine vulnerabilities in Google Chrome for Android. The vulnerabilities are defined in CVE-2022-1633 through CVE-2022-1641 and may enable exploitation via a malcrafted webpage. Successful exploitation may allow the attacker to compromise the user's data on a vulnerable device, and they exist across several components of Chrome.

- CVE-2022-1633: Use after free in Sharesheet.
- CVE-2022-1634: Use after free in Browser UI.
- CVE-2022-1635: Use after free in Permission Prompts.
- CVE-2022-1636: Use after free in Performance APIs.
- CVE-2022-1637: Inappropriate implementation in Web Contents.
- CVE-2022-1638: Heap buffer overflow in V8 Internationalization.
- CVE-2022-1639: Use after free in ANGLE.
- CVE-2022-1640: Use after free in Sharing.
- CVE-2022-1641: Use after free in Web UI Diagnostics.

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 severity and remediation actions that align with their organization's response workflows. As of June 2nd, 2022, Lookout will alert on Chrome versions 101.0.4951.60 or before as vulnerable.

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 nearly 205 million mobile devices and over 170 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

© 2022 Lookout, Inc. LOOKOUT®, the Lookout Shield Design®, LOOKOUT with Shield Design®, SCREAM®, and SIGNAL FLARE® are registered trademarks of Lookout, Inc. in the United States and other countries. EVERYTHING IS OK®, LOOKOUT MOBILE SECURITY®, POWERED BY LOOKOUT®, and PROTECTED BY LOOKOUT® are registered trademarks of Lookout, Inc. in the United States; and POST PERIMETER SECURITY ALLIANCE™ and DAY OF SHECURITY™ are trademarks of Lookout, Inc. All other brand and product names are trademarks or registered trademarks of their respective holders.