**TLP: WHITE**

https://www.cisa.gov/tlp

Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

**DATE(S) ISSUED:**
02/01/2022

**SUBJECT:**
Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code Execution

**OVERVIEW:**
Multiple vulnerabilities have been discovered in Google Chrome, the most severe of which could allow for arbitrary code execution. Google Chrome is a web browser used to access the Internet. Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute arbitrary code in the context of the browser. Depending on the privileges associated with the application, an attacker could view, change, or delete data. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

**THREAT INTELLIGENCE:**
There are no reports that these vulnerabilities are being exploited in the wild.

**SYSTEMS AFFECTED:**
- Google Chrome versions prior to 98.0.4758.80

**RISK:**
**Government:**
- Large and medium government entities: **High**
- Small government entities: **High**

**Businesses:**
- Large and medium business entities: **High**
- Small business entities: **High**

**Home users: Low**

**TECHNICAL SUMMARY:**
Multiple vulnerabilities have been discovered in Google Chrome, the most severe of which could allow for arbitrary code execution. Details of the vulnerabilities are as follows:

- CVE-2022-0452: Use after free in Safe Browsing.
- CVE-2022-0453: Use after free in Reader Mode.
- CVE-2022-0454: Heap buffer overflow in ANGLE.
- CVE-2022-0455: Inappropriate implementation in Full Screen Mode.

- CVE-2022-0456: Use after free in Web Search.
- CVE-2022-0457: Type Confusion in V8.
- CVE-2022-0458: Use after free in Thumbnail Tab Strip.
- CVE-2022-0459: Use after free in Screen Capture.
- CVE-2022-0460: Use after free in Window Dialog.
- CVE-2022-0461: Policy bypass in COOP.
- CVE-2022-0462: Inappropriate implementation in Scroll.
- CVE-2022-0463: Use after free in Accessibility.
- CVE-2022-0464: Use after free in Accessibility.
- CVE-2022-0465: Use after free in Extensions.
- CVE-2022-0466: Inappropriate implementation in Extensions Platform.
- CVE-2022-0467: Inappropriate implementation in Pointer Lock.
- CVE-2022-0468: Use after free in Payments.
- CVE-2022-0469: Use after free in Cast.
- CVE-2022-0470: Out of bounds memory access in V8.

Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute arbitrary code in the context of the browser. Depending on the privileges associated with the application, an attacker could view, change, or delete data. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

**RECOMMENDATIONS:**
The following actions should be taken:
- Apply the stable channel update provided by Google to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

**REFERENCES:**
**Google:**
https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop.html

**CVE:**
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0452
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0453
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0454
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0455
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0456
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0457
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0458
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0459
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0460
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0461
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0462

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0463
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0464
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0465
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0466
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0467
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0468
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0469
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0470