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:
01/19/2022

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 97.0.4692.99

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**
Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**
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-2022-0289: Use after free in Safe browsing.
- CVE-2022-0290: Use after free in Site isolation.
- CVE-2022-0291: Inappropriate implementation in Storage.
- CVE-2022-0292: Inappropriate implementation in Fenced Frames.
- CVE-2022-0293: Use after free in Web packaging.

- CVE-2022-0294: Inappropriate implementation in Push messaging.
- CVE-2022-0295: Use after free in Omnibox.
- CVE-2022-0296: Use after free in Printing.
- CVE-2022-0297: Use after free in Vulkan.
- CVE-2022-0298: Use after free in Scheduling.
- CVE-2022-0300: Use after free in Text Input Method Editor.
- CVE-2022-0301: Heap buffer overflow in DevTools.
- CVE-2022-0302: Use after free in Omnibox.
- CVE-2022-0303: Race in GPU Watchdog.
- CVE-2022-0304: Use after free in Bookmarks.
- CVE-2022-0305: Inappropriate implementation in Service Worker API.
- CVE-2022-0306: Heap buffer overflow in PDFium.
- CVE-2022-0307: Use after free in Optimization Guide.
- CVE-2022-0308: Use after free in Data Transfer.
- CVE-2022-0309: Inappropriate implementation in Autofill.
- CVE-2022-0310: Heap buffer overflow in Task Manager.
- CVE-2022-0311: Heap buffer overflow in Task Manager.

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/2022/01/stable-channel-update-for-desktop_19.html

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0289
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0290
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0291
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0292
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0293
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0294
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0295
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0296

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0297
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0298
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0299
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0300
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0301
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0302
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0303
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0304
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0305
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0306
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0307
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0308
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0309
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0310
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0311