TLP: WHITE
www.cisa.gov/tlp
Information may be distributed without restriction, subject to standard copyright rules.

DATE(S) ISSUED:
03/16/2022

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 99.0.4844.74

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-2022-0971: Use after free in Blink Layout
- CVE-2022-0972: Use after free in Extensions
- CVE-2022-0973: Use after free in Safe Browsing
- CVE-2022-0974: Use after free in Splitscreen
- CVE-2022-0975: Use after free in ANGLE
- CVE-2022-0976: Heap buffer overflow in GPU
- CVE-2022-0977: Use after free in Browser UI
- CVE-2022-0978: Use after free in ANGLE
- CVE-2022-0979: Use after free in Safe Browsing
- CVE-2022-0980: Use after free in New Tab Page

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:
We recommend the following actions 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/2022/03/stable-channel-update-for-desktop_15.html

CVE:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0971

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0972

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0973

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0974

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0975

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0976

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0977

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0978

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0979

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0980