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

DATE(S) ISSUED:
03/27/2022

SUBJECT:
A Vulnerability in Google Chrome Could Allow for Arbitrary Code Execution

OVERVIEW:
A vulnerability has been discovered in Google Chrome that could allow for arbitrary code execution. Google Chrome is a web browser used to access the Internet. Successful exploitation of this vulnerability 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.

THREAT INTELLIGENCE:
Google is aware that an exploit for CVE-2022-1096 exists in the wild.

SYSTEMS AFFECTED:

- Google Chrome versions prior to 99.0.4844.84

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:
A vulnerability has been discovered in Google Chrome, which could allow for arbitrary code execution. Google Chrome is a web browser used to access the Internet. A use after free condition may allow for arbitrary code execution. Successful exploitation of this vulnerability 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.

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_25.html

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1096