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:
10/20/2021

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 currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- Google Chrome versions prior to 95.0.4638.54

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:

- A Heap buffer overflow in Skia. (CVE-2021-37981)
- A Use after free in Incognito. (CVE-2021-37982)
- A Use after free in Dev Tools. (CVE-2021-37983)
- A Heap buffer overflow in PDFium. (CVE-2021-37984)

- A Use after free in V8. (CVE-2021-37985)
- A Heap buffer overflow in Settings. (CVE-2021-37986)
- A Use after free in Network APIs. (CVE-2021-37987)
- A Use after free in Profiles. (CVE-2021-37988)
- An Inappropriate implementation in Blink. (CVE-2021-37989)
- An Inappropriate implementation in WebView. (CVE-2021-37990)
- A Race in V8. (CVE-2021-37991)
- An Out of bounds read in WebAudio. (CVE-2021-37992)
- A Use after free in PDF Accessibility. (CVE-2021-37993)
- An Inappropriate implementation in iFrame Sandbox. (CVE-2021-37994)
- An Inappropriate implementation in WebApp Installer. (CVE-2021-37995)
- An Insufficient validation of untrusted input in Downloads. (CVE-2021-37996)

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/2021/10/stable-channel-update-for-desktop_19.html

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37981
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37982
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37983
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37984
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37985
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37986
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37987
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37988
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37989
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37990
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37991
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37992
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37993
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37994

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37995
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37996