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:
10/29/2021

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:
Google is aware that exploits for CVE-2021-38000 and CVE-2021-38003 exist in the wild.

SYSTEMS AFFECTED:
- Google Chrome versions prior to 95.0.4638.69

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:

- Use after free vulnerability exists in Sign-In. (CVE-2021-37997)
- Use after free vulnerability exists in Garbage Collection. (CVE-2021-37998)
- Insufficient data validation vulnerability exists in New Tab Page. (CVE-2021-37999)
- Insufficient validation of untrusted input vulnerability exists in Intents. (CVE-2021-38000)
- Type Confusion vulnerability exists in V8. (CVE-2021-38001)

- Use after free vulnerability exists in Web Transport. (CVE-2021-38002)
- Inappropriate implementation vulnerability exists in V8. (CVE-2021-38003)

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_28.html

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37997
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37998
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37999
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38000
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38001
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38002
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38003

TLP: WHITE