The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

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:
11/16/2021

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 not aware of any exploits for these vulnerabilities in the wild.

SYSTEMS AFFECTED:
- Google Chrome versions prior to 96.0.4664.45

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 loader (CVE-2021-38005)
- Use after free vulnerability exists in storage foundation (CVE-2021-38006)
- Type Confusion vulnerability exists in V8 (CVE-2021-38007)
- Use after free vulnerability exists in media (CVE-2021-38008)

- Inappropriate implementation vulnerability exists in cache (CVE-2021-38009)
- Inappropriate implementation vulnerability exists in service workers (CVE-2021-38010)
- Use after free vulnerability exists in storage foundation (CVE-2021-38011)
- Type Confusion vulnerability exists in V8 (CVE-2021-38012)
- Heap buffer overflow vulnerability exists in fingerprint recognition (CVE-2021-38013)
- Out of bounds write vulnerability exists in Swiftshader (CVE-2021-38014)
- Inappropriate implementation vulnerability exists in input (CVE-2021-38015)
- Insufficient policy enforcement vulnerability exists in background fetch (CVE-2021-38016)
- Insufficient policy enforcement vulnerability exists in iframe sandbox (CVE-2021-38017)
- Inappropriate implementation vulnerability exists in navigation (CVE-2021-38018)
- Insufficient policy enforcement vulnerability exists in CORS (CVE-2021-38019)
- Insufficient policy enforcement vulnerability exists in contacts picker (CVE-2021-38020)
- Inappropriate implementation vulnerability exists in referrer (CVE-2021-38021)
- Inappropriate implementation vulnerability exists in WebAuthentication (CVE-2021-38022)

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/2021/11/stable-channel-update-for-desktop.html

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38005
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38006
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38007
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38008
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38009
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38010
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38011
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38012
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38013
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38014

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38015
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38016
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38017
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38018
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38019
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38020
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38021
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38022

TLP: WHITE

https://www.cisa.gov/tlp