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
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
01/19/2021

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 88.0.4324.96

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. These vulnerabilities can be exploited if a user visits, or is redirected to, a specially crafted web page. Details of the vulnerabilities are as follows:

- CVE-2020-16044: Use after free in WebRTC.
- CVE-2021-21117: Insufficient policy enforcement in Cryptohome.
- CVE-2021-21118: Insufficient data validation in V8.

- CVE-2021-21119: Use after free in Media.
- CVE-2021-21120: Use after free in WebSQL.
- CVE-2021-21121: Use after free in Omnibox.
- CVE-2021-21122: Use after free in Blink.
- CVE-2021-21123: Insufficient data validation in File System API.
- CVE-2021-21124: Potential user after free in Speech Recognizer.
- CVE-2021-21125: Insufficient policy enforcement in File System API.
- CVE-2021-21126: Insufficient policy enforcement in extensions.
- CVE-2021-21127: Insufficient policy enforcement in extensions.
- CVE-2021-21128: Heap buffer overflow in Blink.
- CVE-2021-21129: Insufficient policy enforcement in File System API.
- CVE-2021-21130: Insufficient policy enforcement in File System API.
- CVE-2021-21131: Insufficient policy enforcement in File System API.
- CVE-2021-21132: Inappropriate implementation in DevTools.
- CVE-2021-21133: Insufficient policy enforcement in Downloads.
- CVE-2021-21134: Incorrect security UI in Page Info.
- CVE-2021-21135: Inappropriate implementation in Performance API.
- CVE-2021-21136: Insufficient policy enforcement in WebView.
- CVE-2021-21137: Inappropriate implementation in DevTools.
- CVE-2021-21138: Use after free in DevTools.
- CVE-2021-21139: Inappropriate implementation in iframe sandbox.
- CVE-2021-21140: Uninitialized Use in USB.
- CVE-2021-21141: Insufficient policy enforcement in File System API.

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:
https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop_19.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+GoogleChromeReleases+%28Google+Chrome+Releases%29

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16044

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21117
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21118
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21119
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21120
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21121
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21122
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21123
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21124
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21125
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21126
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21127
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21128
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21129
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21130
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21131
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21132
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21133
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21134
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21135
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21136
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21137
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21138
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21139
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21140
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21141