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:
03/02/2021

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 89.0.4389.72

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:

- Heap buffer overflow in OpenJPEG. [CVE-2020-27844]
- Heap buffer overflow in TabStrip. [CVE-2021-21159]
- Heap buffer overflow in WebAudio. [CVE-2021-21160]
- Heap buffer overflow in TabStrip. [CVE-2021-21161]

- Use after free in WebRTC. [CVE-2021-21162]
- Insufficient data validation in Reader Mode. [CVE-2021-21163]
- Insufficient data validation in Chrome for iOS. [CVE-2021-21164]
- Object lifecycle issue in audio. [CVE-2021-21165]
- Object lifecycle issue in audio. [CVE-2021-21166]
- Use after free in bookmarks. [CVE-2021-21167]
- Insufficient policy enforcement in appcache. [CVE-2021-21168]
- Out of bounds memory access in V8. [CVE-2021-21169]
- Incorrect security UI in Loader. [CVE-2021-21170]
- Incorrect security UI in TabStrip and Navigation. [CVE-2021-21171]
- Insufficient policy enforcement in File System API. [CVE-2021-21172]
- Side-channel information leakage in Network Internals. [CVE-2021-21173]
- Inappropriate implementation in Referrer. [CVE-2021-21174]
- Inappropriate implementation in Site isolation. [CVE-2021-21175]
- Inappropriate implementation in full screen mode. [CVE-2021-21176]
- Insufficient policy enforcement in Autofill. [CVE-2021-21177]
- Inappropriate implementation in Compositing. [CVE-2021-21178]
- Use after free in Network Internals. [CVE-2021-21179]
- Use after free in tab search. [CVE-2021-21180]
- Side-channel information leakage in autofill. [CVE-2021-21181]
- Insufficient policy enforcement in navigations. [CVE-2021-21182]
- Inappropriate implementation in performance APIs. [CVE-2021-21183]
- Inappropriate implementation in performance APIs. [CVE-2021-21184]
- Insufficient policy enforcement in extensions. [CVE-2021-21185]
- Insufficient policy enforcement in QR scanning. [CVE-2021-21186]
- Insufficient data validation in URL formatting. [CVE-2021-21187]
- Use after free in Blink. [CVE-2021-21188]
- Insufficient policy enforcement in payments [CVE-2021-21189]
- Uninitialized Use in PDFium. [CVE-2021-21190]

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/2021/03/stable-channel-update-for-desktop.html

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27844
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21159
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21160
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21161
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21162
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21163
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21164
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21165
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21166
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21167
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21168
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21169
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21170
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21171
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21172
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21173
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21174
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21175
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21176
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21177
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21178
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21179
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21180
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21181
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21182
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21183
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21184
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21185
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21186
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21187
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21188
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21189
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21190