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:
04/24/2019

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 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 install programs; view, change, or delete data; or create new accounts with full user rights. 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 74.0.3729.108

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 result in 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:

- CORS bypass in Blink. (CVE-2019-5811, CVE-2019-5814)
- CORS bypass in download manager. (CVE-2019-5822)

- Exploit persistence extension on Android. (CVE-2019-5816)
- Forced navigation from service worker. (CVE-2019-5823)
- Heap buffer overflow in Angle on Windows. (CVE-2019-5817)
- Heap buffer overflow in Blink. (CVE-2019-5815)
- Incorrect escaping in developer tools. (CVE-2019-5819)
- Integer overflow in Angle. (CVE-2019-5806)
- Integer overflow in PDFium. (CVE-2019-5820, CVE-2019-5821)
- Memory corruption in V8. (CVE-2019-5807)
- Out of bounds read in V8. (CVE-2019-5813)
- Uninitialized value in media reader. (CVE-2019-5818)
- URL spoof in Omnibox on iOS. (CVE-2019-5812)
- Use after free in Blink. (CVE-2019-5808, CVE-2019-5809)
- Use after free in PDFium. (CVE-2019-5805)
- User information disclosure in Autofill. (CVE-2019-5810)

Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute arbitrary code in the context of the browser, obtain sensitive information, bypass security restrictions and perform unauthorized actions, or cause denial-of-service conditions.

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/2019/04/stable-channel-update-for-desktop_23.html

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5805
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5806
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5807
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5808
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5809
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5810
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5811
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5812
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5813
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5814
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5815
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5816
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5817
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5818

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5819
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5820
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5821
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5822
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5823