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:
06/05/2019

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 75.0.3770.80

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:

- Cross-origin resources size disclosure in Appcache. (CVE-2019-5837)
- Heap buffer overflow in Angle. (CVE-2019-5836)
- Inconsistent security UI placement. (CVE-2019-5833)

- Incorrect CORS handling in XHR. (CVE-2019-5832)
- Incorrect handling of certain code points in Blink. (CVE-2019-5839)
- Incorrectly credentialed requests in CORS. (CVE-2019-5830)
- Incorrect map processing in V8. (CVE-2019-5831)
- Out of bounds read in Swiftshader. (CVE-2019-5835)
- Overly permissive tab access in Extensions. (CVE-2019-5838)
- Popup blocker bypass. (CVE-2019-5840)
- URL spoof in Omnibox on iOS. (CVE-2019-5834)
- Use after free in Download Manager. (CVE-2019-5829)
- Use after free in ServiceWorker. (CVE-2019-5828)

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/2019/06/stable-channel-update-for-desktop.html

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5828
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5829
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5830
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5831
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5832
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5833
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5834
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5835
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5836
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5837
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5838
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5839
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5840

Greg Nohra
Enterprise Security Architect
MS Department of Information Technology Services
601-432-8009 | www.its.ms.gov