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:
07/31/2019

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 76.0.3809.87

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:

- AppCache not robust to compromised renderers. (CVE-2019-5862)
- Click location incorrectly checked. (CVE-2019-5861)
- Comparison of -0 and null yields crash. (CVE-2019-5857)
- Insufficient checks on filesystem (CVE-2019-5856)

- Insufficient filtering of Open URL service parameters. (CVE-2019-5858)
- Insufficient port filtering in CORS for extensions. (CVE-2019-5864)
- Integer overflow in PDFium. (CVE-2019-5855)
- Integer overflow in PDFium text rendering. (CVE-2019-5854)
- Memory corruption in regexp length check. (CVE-2019-5853)
- Object leak of utility functions. (CVE-2019-5852)
- URIs can load alternative browsers. (CVE-2019-5859)
- Site isolation bypass from compromised renderer. (CVE-2019-5865)
- Use-after-free in offline page fetcher. (CVE-2019-5850)
- Use-after-free in PDFium. (CVE-2019-5860)
- Use-after-free in WebUSB on Windows. (CVE-2019-5863)
- Use-after-poison in offline audio context. (CVE-2019-5851)

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/2019/07/stable-channel-update-for-desktop_30.html

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5850
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5851
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5852
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5853
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5854
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5855
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5856
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5857
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5858
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5859
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5860
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5861
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5862
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5863
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5864
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5865

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/

Chris Watts
Security Operations Analyst
MS Department of Information Technology Services
601-432-8201 | www.its.ms.gov