TLP: WHITE
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER:
2018-010

DATE(S) ISSUED:
01/25/2018

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 result in arbitrary code execution. Google Chrome is a web browser used to access the Internet. These vulnerabilities can be exploited if a user visits, or is redirected to, a specially crafted web page. 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.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- Google Chrome prior to 64.0.3282.119

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 these vulnerabilities are as follows:

- Use after free in PDFium. (CVE-2018-6031)
- Same origin bypass in Shared Worker. (CVE-2018-6032)
- Race when opening downloaded files. (CVE-2018-6033)
- Integer overflow in Blink. (CVE-2018-6034)
- Insufficient isolation of devtools from extensions. (CVE-2018-6035, CVE-2018-6045, CVE-2018-6046)
- Integer underflow in WebAssembly. (CVE-2018-6036)
- Insufficient user gesture requirements in autofill. (CVE-2018-6037)
- Heap buffer overflow in WebGL. (CVE-2018-6038)
- XSS in DevTools. (CVE-2018-6039)
- Content security policy bypass. (CVE-2018-6040)
- URL spoof in Navigation. (CVE-2018-6041)
- URL spoof in OmniBox. (CVE-2018-6042, CVE-2018-6050)
- Insufficient escaping with external URL handlers. (CVE-2018-6043)

- Cross origin URL leak in WebGL. (CVE-2018-6047)
- Referrer policy bypass in Blink. (CVE-2018-6048)
- URL spoofing in Omnibox. (CVE-2017-15420)
- UI spoof in Permissions. (CVE-2018-6049)
- Referrer leak in XSS Auditor. (CVE-2018-6051)
- Incomplete no-referrer policy implementation. (CVE-2018-6052)
- Leak of page thumbnails in New Tab Page. (CVE-2018-6053)
- Use after free in WebUI. (CVE-2018-6054)

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:
We recommend the following actions be taken:

- Apply 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/2018/01/stable-channel-update-for-desktop_24.html

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-15420
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6031
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6032
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6033
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6034
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6035
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6036
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6037
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6038
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6039
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6040
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6041
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6042
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6043
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6045
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6046
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6047
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6048
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6049
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6050
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6051
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6052
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6053
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6054

24×7 Security Operations Center
Multi-State Information Sharing and Analysis Center (MS-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722

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/