TLP: WHITE
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER: 2018-140

DATE(S) ISSUED: 12/13/2018

SUBJECT: A Vulnerability in Google Chrome Could Allow for Arbitrary Code Execution

OVERVIEW:
A vulnerability has been discovered in Google Chrome, which could allow for arbitrary code execution. Google Chrome is a web browser used to access the Internet. Successful exploitation of this vulnerability 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 vulnerability 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 71.0.3578.98

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:
A vulnerability has been discovered in Google Chrome, which could allow for arbitrary code execution. This vulnerability is caused by a use-after-free flaw in PDFium (CVE-2018-17481).

Successful exploitation of this vulnerability 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.

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/2018/12/stable-channel-update-for-desktop_12.html

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-17481

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