

**TLP: WHITE**  
**MS-ISAC CYBERSECURITY ADVISORY**

**MS-ISAC ADVISORY NUMBER:**  
2017-103

**DATE(S) ISSUED:**  
10/27/2017

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

**OVERVIEW:**

A vulnerability has been discovered in Google Chrome, which could result in arbitrary code execution. Google Chrome is a web browser used to access the Internet. The vulnerability can be exploited if a user visits, or is redirected to, a specially crafted web page. 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 browser, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Browsers that are configured to have fewer user rights on the system could be less impacted than those that operate with administrative user rights.

**THREAT INTELLIGENCE:**

There are currently no reports of this vulnerability being exploited in the wild.

**SYSTEMS AFFECTED:**

- Google Chrome prior to 62.0.3202.75

**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 result in arbitrary code execution. This vulnerability exists due to a stack overflow condition in V8, which can be exploited if a user visits, or is redirected to, a specially crafted web page. (CVE-2017-15396)

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 browser, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Browsers that are configured to have fewer user rights on the system could be less impacted than those that operate with administrative user rights.

**RECOMMENDATIONS:**

We recommend the following actions be taken:

- Apply appropriate patches 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/2017/10/stable-channel-update-for-desktop\\_26.html](https://chromereleases.googleblog.com/2017/10/stable-channel-update-for-desktop_26.html)

### CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-15396>

24x7 Security Operations Center  
Multi-State Information Sharing and Analysis Center (MS-ISAC)  
31 Tech Valley Drive  
East Greenbush, NY 12061  
[SOC@cisecurity.org](mailto: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/>