

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

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>

DATE(S) ISSUED:

04/29/2015

SUBJECT:

Vulnerability in Google Chrome Could Allow Remote Code Execution

OVERVIEW:

A vulnerability has been discovered in Google Chrome, which could result in remote code execution. Google Chrome is a web browser used to access the Internet. This vulnerability can be exploited if a user visits, or is redirected to, a specially crafted web page. Successful exploitation may allow an attacker to execute arbitrary code in the context of the user running the affected application or result in denial-of-service conditions. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:

There are currently no reports of this vulnerabilities being exploited.

SYSTEM AFFECTED:

- Google Chrome Prior to version 42.0.2311.135

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:

A use-after-free vulnerability exists in the way Google Chrome handles the Domain Object Model (CVE-2015-1243). A use-after-free vulnerability refers to the attempt to access memory after it has been freed, which could result in the execution of malicious code.

An attacker can make use of this vulnerability by directing users to a specially crafted website. Successful exploitation of this vulnerability could result in remote code execution, allowing an attacker to run code in the context of the user running the affected application. Depending on the privileges associated with

the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights

RECOMMENDATIONS:

The following actions should be taken:

- Upgrade to latest versions of Google Chrome 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.

REFERENCES:

Google:

http://googlechromereleases.blogspot.ie/2015/04/stable-channel-update_28.html

Security Focus:

<http://www.securityfocus.com/bid/74389>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1243>

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>