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 ISSUED:
12/9/2015

SUBJECT:
Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Google Chrome, 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 these vulnerabilities could allow an attacker to execute arbitrary code in the context of the browser, obtain sensitive information, bypass security restrictions, or cause denial-of-service conditions.

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

SYSTEM AFFECTED:
- Google Chrome prior to version 47.0.2526.80

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:
Multiple vulnerabilities have been discovered in Google Chrome. These vulnerabilities can be triggered by a user visiting a specially crafted web page. Details of these vulnerabilities are as follows:

- A type-confusion vulnerability exists due to an error in extensions.(CVE-2015-6788)
- A use-after-free vulnerability exists due to an error in Blink.(CVE-2015-6789)
- A security-bypass vulnerability exists due to an escaping issue in saved pages.(CVE-2015-6790)
- Multiple security vulnerabilities exist due to certain unspecified errors. (CVE-2015-6791)

Successful exploitation of these vulnerabilities could allow an attacker to execute arbitrary code in the context of the browser, obtain sensitive information, bypass security restrictions, or cause denial-of-service conditions.

RECOMMENDATIONS:
The following actions should 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.

REFERENCES:
Google:
http://googlechromereleases.blogspot.in/2015/12/stable-channel-update_8.html

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6788
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6789
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6790
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6791

TLP: WHITE
Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.
http://www.us-cert.gov/tlp/