*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:**
09/01/2016

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

**OVERVIEW:**
Multiple vulnerabilities have been discovered in Google Chrome, the most severe of which could result in remote 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 remote 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 53.0.2785.89

**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 remote code execution. These vulnerabilities can be exploited if a user visits, or is redirected to, a specially crafted web page. Details of the vulnerabilities are as follows:

- Universal XSS in Blink. (CVE-2016-5147, CVE-2016-5148)
- Script injection in extensions. (CVE-2016-5149)
- Use after free in Blink. (CVE-2016-5150)
- Use after free in PDFium. (CVE-2016-5151)

- Heap overflow in PDFium. (CVE-2016-5152, CVE-2016-5154, CVE-2016-5157, CVE-2016-5158, CVE-2016-5159.)
- Use after destruction in Blink. (CVE-2016-5153)
- Address bar spoofing. (CVE-2016-5155)
- Use after free in event bindings. (CVE-2016-5156)
- Type confusion in Blink. (CVE-2016-5161)
- Extensions web accessible resources bypass. (CVE-2016-5162)
- Address bar spoofing. (CVE-2016-5163)
- Universal XSS using DevTools. (CVE-2016-5164)
- Script injection in DevTools. (CVE-2016-5165)
- SMB Relay Attack via Save Page As. (CVE-2016-5166)
- Extensions web accessible resources bypass. (CVE-2016-5160)

Successful exploitation of these vulnerabilities could allow an attacker to execute remote 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.com/2016/08/stable-channel-update-for-desktop_31.html

**CVE:**

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5147
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5148
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5149
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5150
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5151
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5152
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5153
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5154
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5155
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5156
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5157
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5158
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5159
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5161
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5162

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5163
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5164
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5165
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5166
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5160