

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.

DATE(S) ISSUED:

11/18/2014

SUBJECT:

Multiple Vulnerabilities in Google Chrome Could Allow for Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in Google Chrome that 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 result in an attacker gaining the same privileges as the user running the affected application. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:

- There is no known proof-of-concept code available at this time.

SYSTEM AFFECTED:

- Google Chrome Prior to 39.0.2171.65

RISK:

Government:

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

Businesses:

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

Home users: High

TECHNICAL SUMMARY:

Multiple Vulnerabilities have been discovered in Google Chrome, and have been patched in the latest Stable Channel Update. This update addressed multiple bug fixes, security updates, and feature enhancements including the following:

- Buffer Overflow Vulnerability CVE-2014-7903
- Buffer Overflow Vulnerability CVE-2014-7904
- Use After Free Remote Code Execution Vulnerability CVE - CVE-2014-7900
- Use After Free Remote Code Execution Vulnerability CVE - CVE-2014-7902
- Unspecified Address Bar Spoofing Vulnerability CVE - CVE-2014-7899
- Integer Overflow Vulnerability CVE - CVE-2014-7908
- Unspecified Security Vulnerability CVE - CVE-2014-7905
- Information Disclosure Vulnerability CVE - CVE-2014-7909
- Integer Overflow Vulnerability CVE - CVE-2014-7901
- Multiple Security Vulnerabilities CVE - CVE-2014-7910
- Use After Free Remote Code Execution Vulnerability CVE - CVE-2014-7906
- Use After Free Remote Code Execution Vulnerability CVE - CVE-2014-7907

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:

Security Focus:

<http://www.securityfocus.com/bid/71164>

<http://www.securityfocus.com/bid/71166>

<http://www.securityfocus.com/bid/71163>

<http://www.securityfocus.com/bid/71165>

<http://www.securityfocus.com/bid/71160>

<http://www.securityfocus.com/bid/71168>

<http://www.securityfocus.com/bid/71162>

<http://www.securityfocus.com/bid/71167>

<http://www.securityfocus.com/bid/71158>

<http://www.securityfocus.com/bid/71161>

<http://www.securityfocus.com/bid/71159>

<http://www.securityfocus.com/bid/71170>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7903>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7904>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7900>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7902>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7899>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7908>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7905>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7909>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7901>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7910>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7906>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7907>

Google:

http://googlechromereleases.blogspot.in/2014/11/stable-channel-update_18.html

<http://googlechromereleases.blogspot.in/2014/11/stable-channel-update.html>