

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:

01/22/2015

SUBJECT:

Multiple Vulnerabilities in Google Chrome Could Allow for Remote Code Execution

EXECUTIVE SUMMARY:

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 40.0.2214.91

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:

- Memory corruption in ICU [CVE-2014-7923]
- Use-after-free in IndexedDB. [CVE-2014-7924]
- Use-after-free in WebAudio. [CVE-2014-7925]
- Memory corruption in ICU. [CVE-2014-7926]
- Memory corruption in V8. [CVE-2014-7927]
- Memory corruption in V8. [CVE-2014-7928]
- Use-after-free in DOM. [CVE-2014-7929]
- Use-after-free in DOM. [CVE-2014-7930]

- Memory corruption in V8. [CVE-2014-7931]
- Use-after-free in DOM. [CVE-2014-7932]
- Use-after-free in FFmpeg. [CVE-2014-7933]
- Use-after-free in DOM. [CVE-2014-7934]
- Use-after-free in Speech. [CVE-2014-7935]
- Use-after-free in Views. [CVE-2014-7936]
- Use-after-free in FFmpeg. [CVE-2014-7937]
- Memory corruption in Fonts. [CVE-2014-7938]
- Same-origin-bypass in V8. [CVE-2014-7939]
- Uninitialized-value in ICU. [CVE-2014-7940]
- Out-of-bounds read in UI. [CVE-2014-7941]
- Uninitialized-value in Fonts. [CVE-2014-7942]
- Out-of-bounds read in Skia. [CVE-2014-7943]
- Out-of-bounds read in PDFium. [CVE-2014-7944]
- Out-of-bounds read in PDFium. [CVE-2014-7945]
- Out-of-bounds read in Fonts. [CVE-2014-7946]
- Out-of-bounds read in PDFium. [CVE-2014-7947]
- Caching error in AppCache. [CVE-2014-7948]
- Various fixes from internal audits, fuzzing and other initiatives. [CVE-2015-1205]

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:

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7923>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7924>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7925>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7926>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7927>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7928>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7929>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7930>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7931>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7932>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7933>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7934>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7935>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7936>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7937>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7938>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7939>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7940>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7941>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7942>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7943>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7944>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7945>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7946>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7947>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7948>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1205>

Google:

<http://googlechromereleases.blogspot.com/2015/01/stable-update.html>