

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:

05/20/2015

SUBJECT:

Multiple Vulnerabilities in Google Chrome Could Allow Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in Google Chrome, 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 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 these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- Google Chrome Prior to 43.0.2357.65

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:

Twelve 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:

- Sandbox escape in Chrome (CVE-2015-1252)
- Cross-origin bypass in DOM (CVE-2015-1253)

- Cross-origin bypass in Editing (CVE-2015-1254)
- Use-after-free in WebAudio (CVE-2015-1255)
- Use-after-free in SVG (CVE-2015-1256)
- Use-after-free in Speech (CVE-2015-1251)
- Container-overflow in SVG (CVE-2015-1257)
- Negative-size parameter in Libvpx (CVE-2015-1258)
- Uninitialized value in PDFium (CVE-2015-1259)
- Use-after-free in WebRTC (CVE-2015-1260)
- URL bar spoofing (CVE-2015-1261)
- Uninitialized value in Blink (CVE-2015-1262)
- Insecure download of spellcheck dictionary (CVE-2015-1263)
- Cross-site scripting in bookmarks (CVE-2015-1264)

Successful exploitation of these vulnerabilities could allow an attacker to execute arbitrary code in the context of the browser. Depending on the privileges afforded to the browser, an attacker can bypass security restrictions, or cause denial-of-service conditions; other attacks may also be possible.

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 Chrome:

http://googlechromereleases.blogspot.ie/2015/05/stable-channel-update_19.html

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1251>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1252>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1253>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1254>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1255>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1256>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1257>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1258>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1259>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1260>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1261>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1262>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1263>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1264>

TLP: WHITE

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

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