

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:

04/17/2015

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. Attackers can exploit these issues 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.

THREAT INTELLIGENCE:

There are currently no reports of these vulnerabilities being exploited in the wild

SYSTEM AFFECTED:

- Google Chrome Prior to version 42.0.2311.90

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:

Thirteen 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:

- Cross-origin bypass in the HTML parser (CVE-2015-1235)
- Cross-origin bypass in Blink (CVE-2015-1236)
- Use-after-free in IPC (CVE-2015-1237)
- Out-of-bounds write error in Skia (CVE-2015-1238)
- Out-of-bounds read error in WebGL (CVE-2015-1240)
- Tap-Jacking attack (CVE-2015-1241)
- Type Confusion attack in V8 (CVE-2015-1242)
- HSTS bypass attack in WebSockets (CVE-2015-1244)
- Use-after free in PDFium (CVE-2015-1245)
- Out-of-bounds read error in Blink (CVE-2015-1246)
- Scheme issues flaw in OpenSearch (CVE-2015-1247)
- SafeBrowsing bypass attack (CVE-2015-1248)
- Multiple vulnerabilities were fixed in V8, the JavaScript engine in use by Google Chrome (CVE-2015-1249)

Successful exploitation 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/2015/04/stable-channel-update_14.html

Security Focus:

<http://www.securityfocus.com/bid/74165>

<http://www.securityfocus.com/bid/74167>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1235>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1236>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1237>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1238>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1240>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1241>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1242>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1244>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1245>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1246>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1247>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1248>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1249>

TLP: WHITE

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

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