

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
MS-ISAC CYBER SECURITY ADVISORY

DATE ISSUED:

07/22/2015

SUBJECT:

Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary 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 of these vulnerabilities could allow an attacker to execute arbitrary code, in the context of the browser or obtain sensitive information. 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.

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. There are known proof-of-concept exploits for this vulnerability.

SYSTEM AFFECTED:

- Google Chrome Prior to 44.0.2403.89

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:

Multiple 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:

- Heap-buffer-overflow in pdfium (CVE-2015-1271)
- Heap-buffer-overflow in pdfium (CVE-2015-1273)
- Settings allowed executable files to run immediately after download (CVE-2015-1274)
- UXSS in Chrome for Android (CVE-2015-1275)
- Use-after-free in IndexedDB (CVE-2015-1276)
- Heap-buffer-overflow in pdfium (CVE-2015-1279)
- Memory corruption in skia (CVE-2015-1280)
- CSP bypass (CVE-2015-1281)
- Use-after-free in pdfium (CVE-2015-1282)
- Heap-buffer-overflow in expat (CVE-2015-1283)

- Use-after-free in blink (CVE-2015-1284)
- UXSS in blink (CVE-2015-1286)
- SOP bypass with CSS (CVE-2015-1287)
- Uninitialized memory read in ICU (CVE-2015-1270)
- Use-after-free related to unexpected GPU process termination (CVE-2015-1272)
- Use-after-free in accessibility (CVE-2015-1277)
- URL spoofing using pdf files (CVE-2015-1278)
- Information leak in XSS auditor (CVE-2015-1285)
- Spell checking dictionaries fetched over HTTP (CVE-2015-1288)
- Various fixes from internal audits, fuzzing and other initiatives (CVE-2015-1289)

Successful exploitation of these vulnerabilities could allow an attacker to execute arbitrary code, in the context of the browser or obtain sensitive information. 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:

http://googlechromereleases.blogspot.com/2015/07/stable-channel-update_21.html

CVE:

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1270>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1271>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1272>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1273>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1274>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1275>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1276>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1277>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1278>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1279>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1280>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1281>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1282>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1283>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1284>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1285>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1286>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1287>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1288>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1289>

TLP: WHITE

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

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