

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:

8/26/2014

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 not any known proof-of-concept code available at this time.

SYSTEM AFFECTED:

- Google Chrome Prior to 37.0.2062.94

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:

Eight unspecified vulnerabilities were patched in the latest version of Google Chrome. They are listed as follows:

- Use-after-free vulnerability in SVG that could result in remote code execution. [CVE-2014-3168]
- Use-after-free vulnerability in DOM that could result in remote code execution. [CVE-2014-3169]
- Extension permission dialog spoofing. [CVE-2014-3170]
- Use-after-free vulnerability in bindings that could result in remote code execution. [CVE-2014-3171]
- Unspecified security vulnerability related to extension debugging. [CVE-2014-3172]
- Information disclosure vulnerability related to uninitialized memory read in WebGL. [CVE-2014-3173]
- Uninitialized memory read in Web Audio. [CVE-2014-3174]
- Various fixes from internal audits. [CVE-2014-3175]
- Multiple unspecified remote code execution vulnerabilities [CVE-2014-3176]

RECOMMENDATIONS:

The following actions should be taken:

- Update vulnerable Google Chrome products immediately after appropriate testing by following the steps outlined by Google.
- 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.
- Do not open email attachments or click on URLs from unknown or un-trusted sources.

REFERENCES:

Google:

<http://googlechromereleases.blogspot.com/2014/08/stable-channel-update.html>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3168>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3169>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3170>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3171>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3172>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3173>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3174>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3175>

SecurityFocus:

<http://www.securityfocus.com/bid/69398>

<http://www.securityfocus.com/bid/69403>

<http://www.securityfocus.com/bid/69405>

<http://www.securityfocus.com/bid/69404>

<http://www.securityfocus.com/bid/69407>

<http://www.securityfocus.com/bid/69400>

<http://www.securityfocus.com/bid/69406>

<http://www.securityfocus.com/bid/69401>

<http://www.securityfocus.com/bid/69402>