

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:

3/13/2015

SUBJECT:

Multiple Vulnerabilities in Google Chrome Could Allow for Remote Code Execution

OVERVIEW:

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

SYSTEM AFFECTED:

- Google Chrome before 40.0.2214.91

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:

Google Chrome is prone to multiple vulnerabilities that could allow for remote code execution. These vulnerabilities are as follows:

- Multiple buffer-overflow vulnerabilities related to intra-object-overflow issues in PDFium. These issues occur due to multiple off-by-one errors in the 'fpdfapi/fpdf_font/font_int.h' in PDFium. (CVE 2015-1359)
- A buffer-overflow vulnerability that occurs due to an unspecified error in Skia. This issue occurs because it fails to properly handle specially crafted data during text drawing. (CVE 2015 -1360)

Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. 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 access. Failed exploit attempts could result in a denial-of-service condition.

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:

SecurityFocus:

<http://www.securityfocus.com/advisories/34848>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1359>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1360>

TLP: WHITE

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

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