

*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:**

3/27/2013

**SUBJECT:**

Multiple Security Vulnerabilities in Google Chrome Could Allow Remote Code Execution

**OVERVIEW:**

Multiple vulnerabilities in Google Chrome could allow an attacker to execute arbitrary code in the context of the browser, cause denial-of-service conditions, and bypass security restrictions; other attacks may also be possible. Google Chrome is a web browser used to access the Internet. Attackers can exploit these issues to execute arbitrary code in the context of the browser, cause denial-of-service conditions, and bypass security restrictions; other attacks may also be possible.

Successful exploitation of these vulnerabilities may result in either an attacker gaining the same privileges as the logged on user, or gaining session authentication credentials. 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.

**SYSTEMS AFFECTED:**

- Google Chrome Prior to 26.0.1410.43

**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**

**DESCRIPTION:**

Multiple vulnerabilities have been discovered in Google Chrome. Details of these vulnerabilities are as follows:

- A use-after-free issue in Web Audio. [CVE-2013-0916]
- An out-of-bounds read issue in the URL loader. [CVE-2013-0917]
- A security issue in dev tools navigation during drag and drop. [CVE-2013-0918]
- A use-after-free issue with pop-up windows in extensions. [CVE-2013-0919]
- A use-after-free issue in extension bookmarks API. [CVE-2013-0920]
- A security issue because it fails to ensure isolated web sites run in their own processes. [CVE-2013-0921]
- A security issue because it fails to avoid HTTP basic authentication brute force attacks.[CVE-2013-0922]
- A security issue due to memory safety errors in the USB Apps API. [CVE-2013-0923]
- A security issue because it fails to properly check an extensions permissions API usage. [CVE-2013-0924]
- A security issue because it fails to properly restrict the URLs leakage to the extensions without the tabs permissions. [CVE-2013-0925]
- A security issue because it fails to restrict active tags pasting in certain circumstances. [CVE-2013-0926]

Successful exploitation of some of the above vulnerabilities could result in an attacker gaining the same privileges as the user. Depending on the privileges associated with the user, an attacker could install programs; view, change, delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

## **RECOMMENDATIONS:**

The following actions should be taken:

- Update vulnerable Google Chrome products immediately after appropriate testing by following the steps outlined by Google here: <http://support.google.com/chrome/bin/answer.py?hl=en&answer=95414>
- Run all software as a non-privileged user with minimal access rights.
- Ensure that all non-administrative tasks, such as browsing the web and reading email, are performed as an unprivileged user with minimal access rights.
- Deploy network intrusion detection systems to monitor network traffic for malicious activity.
- Do not follow links provided by unknown or untrusted sources.
- To prevent a successful exploit of script-execution vulnerabilities, disable support for script code and active content within the client browser. Note that this tactic might adversely affect websites that rely on HTML or script code.

- Various memory-protection schemes (such as non-executable and randomly mapped memory segments) may hinder an attacker's ability to exploit memory corruption vulnerabilities.

## REFERENCES:

### Google

<http://www.google.com/chrome>

[http://googlechromereleases.blogspot.ie/2013/03/stable-channel-update\\_26.html](http://googlechromereleases.blogspot.ie/2013/03/stable-channel-update_26.html)

### Security Focus:

<http://www.securityfocus.com/bid/58712>

<http://www.securityfocus.com/bid/58723>

<http://www.securityfocus.com/bid/58724>

<http://www.securityfocus.com/bid/58725>

<http://www.securityfocus.com/bid/58727>

<http://www.securityfocus.com/bid/58729>

<http://www.securityfocus.com/bid/58731>

### CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0916>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0917>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0918>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0919>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0920>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0921>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0922>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0923>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0924>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0925>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0926>