

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:

02/22/2013

SUBJECT:

Multiple Google Chrome Vulnerabilities Could Allow for Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in Google Chrome that could allow remote code execution, the bypass of security restrictions, or cause denial-of-service conditions. Google Chrome is a web browser used to access the Internet. Details are not currently available that depict accurate attack scenarios, but it is believed that some of the vulnerabilities can likely be exploited if a user visits, or is redirected to a specially crafted web page.

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.

SYSTEM AFFECTED:

- Google Chrome for Windows and Linux versions prior to 25.0.1364.97
- Google Chrome for Mac versions prior to 25.0.1364.99

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 memory-corruption with web audio nodes. [CVE-2013-0879]
- A use-after-free error exists in database handling. [CVE-2013-0880]
- A security issue that occurs due to a bad read in Matroska handling. [CVE-2013-0881]
- A security issue due to bad memory access with excessive SVG parameters. [CVE-2013-0882]
- A security issue due to a bad read in Skia. [CVE-2013-0883]
- A security issue due to an inappropriate load of NaCl. [CVE-2013-0884]
- A security issue because too many API permissions are granted to the web store. [CVE-2013-0885]
- A security issue exists due to incorrect NaCl signal handling. [CVE-2013-0886]
- A security issue occurs because the developer tools process has too many permissions and places too much trust in the connected server. [CVE-2013-0887]
- An out-of-bounds read issue in Skia. [CVE-2013-0888]
- A security issue that occurs due to a tighten user gesture check for dangerous file downloads. [CVE-2013-0889]
- Multiple memory-corruption issues exist across the IPC layer. [CVE-2013-0890]
- An integer-overflow vulnerability occurs when handling blob. [CVE-2013-0891]
- Multiple security weakness exist across the IPC layer.[CVE-2013-0892]
- A race-condition vulnerability occurs when handling media.[CVE-2013-0893]
- A buffer-overflow vulnerability exists in vorbis decoding. [CVE-2013-0894]
- A security issue exist due to incorrect path handling while copying a file. [CVE-2013-0895]
- Multiple security issues occurs due to memory management when handling a plug-in message. [CVE-2013-0896]

- An off-by-one read issue exists in PDF. [CVE-2013-0897]
- A use-after-free issue occurs when handling a URL. [CVE-2013-0898]
- An integer-overflow vulnerability occurs when handling Opus. [CVE-2013-0899]
- A race-condition vulnerability exists in ICU. [CVE-2013-0900]

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 (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites, follow links, or open files provided by unknown or un-trusted sources.

REFERENCES:

Security Focus:

<http://www.securityfocus.com/bid/58101>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0879>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0880>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0881>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0882>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0883>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0884>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0885>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0886>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0887>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0888>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0889>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0890>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0891>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0892>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0893>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0894>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0895>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0896>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0897>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0898>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0899>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0900>