



**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory**

November 12, 2013

The following cyber advisory was issued by the State of Alaska and was 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.

ADVISORY NUMBER:

SA2013-088

DATE(S) ISSUED:

11/12/2013

SUBJECT:

Multiple Vulnerabilities in Google Chrome Could Allow Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in Google Chrome that could allow remote code execution or cause denial-of-service conditions. 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 may result in an attacker gaining the same privileges as the logged on user. 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 31.0.1650.48

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 vulnerability has been which affects the following:
 - o Media Elements [CVE-2013-6622]
 - o Speech Input Elements [CVE-2013-6621]
 - o DOM Ranges [CVE-2013-6625]
 - o Libjingle [CVE-2013-6631]
 - o 'id' Attribute String [CVE-2013-6624]
- A memory corruption vulnerability that occurs due to an out-of-bounds read error in HTTP parsing. [CVE-2013-6627]
- A memory corruption vulnerability that occurs due to an out-of-bounds read error in SVG. [CVE-2013-6623]

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:

We recommend the following actions 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/2013/11/stable-channel-update.html>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-6621>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-6622>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-6623>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-6624>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-6625>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-6627>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-6631>

SecurityFocus:

<http://www.securityfocus.com/bid/63667>

<http://www.securityfocus.com/bid/63669>

<http://www.securityfocus.com/bid/63670>

<http://www.securityfocus.com/bid/63671>

<http://www.securityfocus.com/bid/63672>

<http://www.securityfocus.com/bid/63673>

<http://www.securityfocus.com/bid/63675>