



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

May 23, 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:

SA2013-047

DATE(S) ISSUED:

05/22/2013

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, 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 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, Mac and Linux versions prior to 27.0.1453.93

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 SVG. [CVE-2013-2837]
- An out-of-bounds read issue in v8. [CVE-2013-2838]
- A security vulnerability exists due to bad cast in clipboard handling. [CVE-2013-2839]
- A use-after-free issue in media loader. [CVE-2013-2840]
- A use-after-free issue in pepper resource handling. [CVE-2013-2841]
- A use-after-free issue in widget handling. [CVE-2013-2842]
- A use-after-free issue in speech handling. [CVE-2013-2843]
- A use-after-free issue in style resolution. [CVE-2013-2844]
- A memory-corruption vulnerability exists in Web Audio. [CVE-2013-2845]
- A use-after-free issue in media loader. [CVE-2013-2846]
- A use-after-free race condition issue with workers. [CVE-2013-2847]
- An information-disclosure issue with XSS Auditor. [CVE-2013-2848]
- A cross-site scripting issue with drag+drop or copy+paste. [CVE-2013-2849]
- Various fixes from internal audits, fuzzing and other initiatives. [CVE-2013-2836]

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 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 or follow links provided by unknown or un-trusted sources.
- Do not open email attachments or click on URLs from unknown or untrusted sources.

REFERENCES:

Security Focus:

<http://www.securityfocus.com/bid/60056>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2836>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2837>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2838>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2839>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2840>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2841>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2842>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2843>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2844>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2845>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2846>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2847>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2848>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2849>

Google:

<http://googlechromereleases.blogspot.ie/2013/05/stable-channel-release.html>