



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

January 21, 2016

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:
SA2016-016**

**DATE(S) ISSUED:
01/21/2016**

**SUBJECT:
Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code Execution**

**OVERVIEW:
Multiple vulnerabilities have been discovered in Google Chrome, which could result in arbitrary 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 allow an attacker to execute arbitrary code in the context of the browser, obtain sensitive information, bypass security restrictions, or cause denial-of-service conditions.**

**THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.**

SYSTEM AFFECTED:

•Google Chrome prior to version 48.0.2564.82

•V8 versions prior to 4.8.271.17

RISK:

Government:

- Large and medium government entities: High
- Small government entities: Medium

Businesses:

- Large and medium business entities: High
- Small business entities: Medium

Home users: Low

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in Google Chrome. These vulnerabilities can be triggered by a user visiting a specially crafted web page.

Details of these vulnerabilities are as follows:

- A bad cast vulnerability in V8 (CVE-2016-1612)
- A use-after-free vulnerability in PDFium (CVE-2016-1613)
- An information leakage vulnerability in Blink (CVE-2016-1614)
- An origin confusion vulnerability in Omnibox (CVE-2016-1615)
- A URL spoofing vulnerability (CVE-2016-1616)
- A vulnerability in History that allowed sniffing with HSTS and CSP (CVE-2016-1617)
- Weak random number generation in Blink (CVE-2016-1618)
- An out-of-bounds read vulnerability in PDFium (CVE-2016-1619)
- Various fixes from internal audits, fuzzing and other initiatives (CVE-2016-1620)
- Multiple other vulnerabilities in V8

Successful exploitation of these vulnerabilities could allow an attacker to execute arbitrary code in the context of the browser, obtain sensitive information, bypass security restrictions, or cause denial-of-service conditions.

RECOMMENDATIONS:

We recommend the following actions 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:

Google:

http://googlechromereleases.blogspot.com/2016/01/stable-channel-update_20.html

CVE:

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1612>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1613>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1614>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1615>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1616>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1617>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1618>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1619>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1620>