

**DATE(S) ISSUED:**

10/11/2013

**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, bypass of security restrictions, spoof the displayed uniform resource identifier URI in the address bar, 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.

**SYSTEMS AFFECTED:**

- Google Chrome Prior to 30.0.1599.66

**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 security vulnerability exists due to races in web audio. [CVE-2013-2906]
- An out-of-bounds read error in 'Window.prototype' object. [CVE-2013-2907]
- Multiple address bar spoofing vulnerabilities exists related to the '204 No Content?' status code. [CVE-2013-2908] and [CVE-2013-2916]
- A use-after-free issue in inline-block rendering. [CVE-2013-2909]
- A use-after-free issue in Web Audio. [CVE-2013-2910]
- A use-after-free issue in XSLT. [CVE-2013-2911]
- A use-after-free issue in PPAPI. [CVE-2013-2912]

- A use-after-free issue in XML document parsing. [CVE-2013-2913]
- A use-after-free issue in the Windows color chooser dialog. [CVE-2013-2914]
- An address bar spoofing vulnerability occurs through a malformed scheme. [CVE-2013-2915]
- An out-of-bounds read error in web audio. [CVE-2013-2917]
- A use-after-free issue in Dom. [CVE-2013-2918]
- A memory-corruption vulnerability exists in V8. [CVE-2013-2919]
- An out-of-bounds read error in URL parsing. [CVE-2013-2920]
- A use-after-free issue in resource loader. [CVE-2013-2921]
- A use-after-free issue in template element. [CVE-2013-2922]
- Multiple unspecified issues affect the application. [CVE-2013-2923]
- A use-after-free in ICU. [CVE-2013-2924]

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.
- 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/2013/10/stable-channel-update.html>

##### **CVE:**

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2906>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2907>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2908>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2909>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2910>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2911>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2912>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2913>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2914>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2915>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2916>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2917>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2918>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2919>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2920>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2921>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2922>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2923>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2924>

**SecurityFocus:**

<http://www.securityfocus.com/bid/62752>