



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

**April 30, 2014**

*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:**

SA2014-034

**DATE(S) ISSUED:**

04/30/2014

**SUBJECT:**

Multiple Vulnerabilities in Mozilla Products Could Allow Remote Code Execution

**EXECUTIVE SUMMARY:**

Multiple vulnerabilities have been discovered in Mozilla Firefox, Thunderbird, and SeaMonkey applications, which could allow remote code execution. Mozilla Firefox is a web browser used to access the Internet. Mozilla Thunderbird is an email client. Mozilla SeaMonkey is a cross platform Internet suite of tools ranging from a web browser to an email client. Successful exploitation of these vulnerabilities could 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.

**THREAT INTELLIGENCE:**

At this time, there is no known proof-of-concept code available.

**SYSTEMS AFFECTED:**

- Firefox versions prior to 29
- Firefox Extended Support Release (ESR) versions prior to 24.5
- Thunderbird versions prior to 24.5
- SeaMonkey versions prior to 2.26

**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

#### **TECHNICAL SUMMARY:**

Fifteen vulnerabilities have been reported in various Mozilla products. Details of the vulnerabilities are as follows:

- Two memory-corruption vulnerabilities affect the browser engine. [CVE-2014-1518, CVE-2014-1519]
- A local privilege-escalation vulnerability in the 'Mozilla Maintenance Service' installer. Specifically this issue occurs because it writes to a temporary directory created during the update process which is writable by users. [CVE-2014-1520]
- A memory corruption vulnerability exists due to an out of bounds read in the mozilla::dom::OscillatorNodeEngine::ComputeCustom Web Audio function. [CVE-2014-1522]
- An out of bounds vulnerability exists due to a read while decoding JPG images because of a failure to sufficiently bounds-check user-supplied data. [CVE-2014-1523]
- A buffer overflow vulnerability exists when using non-XBL object as XBL because the XBL status of the object is not properly validated. [CVE-2014-1524]
- A use-after-free vulnerability exists in the Text Track Manager for HTML video. [CVE-2014-1525]
- A vulnerability exists in Firefox for Android that allows an attacker to suppress the address bar after it has been scrolled off the screen through the use of script interacting DOM events. [CVE-2014-1527] Note: This issue affects Firefox on Android systems.
- An out-of-bounds vulnerability exists when writing in the Cairo graphics library in certain circumstances. [CVE-2014-1528]
- A privilege escalation vulnerability exists where sites that have been given notification permissions by a user can bypass security checks on source components of the Web Notification API. [CVE-2014-1529]
- A cross-site scripting (XSS) vulnerability exists using the browser history navigations to load a website, although the URI in the address bar would be incorrect. [CVE-2014-1530]
- A use-after-free vulnerability exists in which the imgLoader object is freed while resizing images. [CVE-2014-1531]
- The Network Security Services (NSS) library does not handle IDNA domain prefixes for wildcard certificates. This leads to improper matching of domains when they should not be matched. [CVE-2014-1492]
- A use-after-free vulnerability exists during host resolution handled by nsHostResolver. [CVE-2014-1532]
- The debugger can bypass XrayWrappers with JavaScript that may lead to privilege escalation. [CVE-2014-1526]

Successful exploitation could result in an attacker gaining the same privileges as the affected application. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or 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 Mozilla products immediately after appropriate testing.
- 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.

- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

## REFERENCES:

### Mozilla:

<http://www.mozilla.org/security/announce/2014/mfsa2014-34.html>  
<http://www.mozilla.org/security/announce/2014/mfsa2014-35.html>  
<http://www.mozilla.org/security/announce/2014/mfsa2014-36.html>  
<http://www.mozilla.org/security/announce/2014/mfsa2014-37.html>  
<http://www.mozilla.org/security/announce/2014/mfsa2014-38.html>  
<http://www.mozilla.org/security/announce/2014/mfsa2014-39.html>  
<http://www.mozilla.org/security/announce/2014/mfsa2014-40.html>  
<http://www.mozilla.org/security/announce/2014/mfsa2014-41.html>  
<http://www.mozilla.org/security/announce/2014/mfsa2014-42.html>  
<http://www.mozilla.org/security/announce/2014/mfsa2014-43.html>  
<http://www.mozilla.org/security/announce/2014/mfsa2014-44.html>  
<http://www.mozilla.org/security/announce/2014/mfsa2014-45.html>  
<http://www.mozilla.org/security/announce/2014/mfsa2014-46.html>  
<http://www.mozilla.org/security/announce/2014/mfsa2014-47.html>

### CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1518>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1519>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1520>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1522>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1523>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1524>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1525>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1527>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1528>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1529>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1530>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1531>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1492>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1532>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1526>

### SecurityFocus:

<http://www.securityfocus.com/bid/67137>  
<http://www.securityfocus.com/bid/67136>  
<http://www.securityfocus.com/bid/67135>  
<http://www.securityfocus.com/bid/67134>  
<http://www.securityfocus.com/bid/67133>  
<http://www.securityfocus.com/bid/67132>  
<http://www.securityfocus.com/bid/67131>  
<http://www.securityfocus.com/bid/67130>  
<http://www.securityfocus.com/bid/67129>  
<http://www.securityfocus.com/bid/67128>  
<http://www.securityfocus.com/bid/67127>  
<http://www.securityfocus.com/bid/67126>  
<http://www.securityfocus.com/bid/67125>  
<http://www.securityfocus.com/bid/67123>  
<http://www.securityfocus.com/bid/66356>