

*The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is 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.*

**DATE(S) ISSUED:**

06/11/2014

**SUBJECT:**

Multiple Vulnerabilities in Mozilla Products Could Allow Remote Code Execution

**EXECUTIVE SUMMARY:**

Multiple vulnerabilities have been discovered in Mozilla Firefox, Thunderbird, and Netscape portable runtime applications, which could allow remote code execution. Mozilla Firefox is a web browser used to access the Internet. Mozilla Thunderbird is an email client. Netscape portable runtime (NSPR) is a platform abstraction library. 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:**

Currently there are no known exploits regarding these vulnerabilities.

**SYSTEMS AFFECTED:**

- Firefox versions prior to 30
- Firefox Extended Support Release (ESR) versions prior to 24.6
- Thunderbird versions prior to 24.6
- Netscape Portable Runtime versions prior to 4.10.6

**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:**

Eight vulnerabilities have been reported for various Mozilla products. Details of the vulnerabilities are as follows:

- Multiple memory-corruption vulnerabilities affect the browser engine. [CVE-2014-1533] [MFSA-2014-48]
- Multiple use-after-free and out of bound read vulnerabilities affecting the browser engine. [CVE-2014-1536] [CVE-2014-1537] [MFSA-2014-49]
- Cursor rendering issue can occur after flash issue, causing the cursor to appear to be invisible. This issue only affects OS X. [CVE-2014-1539] [MFSA-2014-50]
- A use-after-free vulnerability was discovered in the Event Listener Manager. [CVE-2014-1540] [MFSA-2014-51]
- A use-after-free vulnerability was discovered in the SMIL Animation Controller. [CVE-2014-1541] [MFSA-2014-52]
- A buffer overflow vulnerability was discovered in the Web Audio Speex resampler. [CVE-2014-1542] [MFSA-2014-53]
- A buffer overflow vulnerability was discovered in the Gamepad API. [CVE-2014-1543] [MFSA-2014-54]
- A out of bounds write vulnerability was discovered in the Netscape Portable Runtime (NSPR). [CVE-2014-1545] [MFSA-2014-55]

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:**

The following actions should 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/mfsa2014-48.html>

<http://www.mozilla.org/security/announce/2014/mfsa2014-49.html>

<http://www.mozilla.org/security/announce/2014/mfsa2014-50.html>

<http://www.mozilla.org/security/announce/2014/mfsa2014-51.html>

<http://www.mozilla.org/security/announce/2014/mfsa2014-52.html>

<http://www.mozilla.org/security/announce/2014/mfsa2014-53.html>

<http://www.mozilla.org/security/announce/2014/mfsa2014-54.html>

<http://www.mozilla.org/security/announce/2014/mfsa2014-55.html>

**CVE:**

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1533>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1536>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1537>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1539>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1540>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1541>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1542>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1543>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1545>

**SecurityFocus:**

<http://www.securityfocus.com/bid/67964>

<http://www.securityfocus.com/bid/67965>

<http://www.securityfocus.com/bid/67966>

<http://www.securityfocus.com/bid/67967>

<http://www.securityfocus.com/bid/67971>

<http://www.securityfocus.com/bid/67975>

<http://www.securityfocus.com/bid/67976>

<http://www.securityfocus.com/bid/67978>

<http://www.securityfocus.com/bid/67979>