

*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:**

9/2/2014

**SUBJECT:**

Multiple Vulnerabilities in Mozilla Firefox and Thunderbird Could Allow for Remote Code Execution

**EXECUTIVE SUMMARY:**

Multiple vulnerabilities have been identified in Mozilla Firefox and Thunderbird that could allow for remote code execution. Mozilla Firefox is a web browser used to access the Internet and Mozilla Thunderbird is an email client. Successful exploitation of these vulnerabilities could result in 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**

There are currently no reports of these vulnerabilities being exploited in the wild.

**SYSTEM AFFECTED:**

- Mozilla Firefox
- Mozilla Firefox Extended Support Release (ESR)
- Mozilla Thunderbird

**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:**

Six vulnerabilities have been reported in Mozilla Firefox and Thunderbird. Details of the vulnerabilities are as follows:

- An information-disclosure vulnerability exists because the application fails to properly handle specially crafted GIF image. An attacker can exploit this issue to disclose sensitive information through uninitialized memory. [CVE-2014-1564, MFSA 2014-69]
- A use-after-free memory-corruption vulnerability that occurs due to an error in text layout when interacting with the setting of text directionality. [CVE-2014-1567, MFSA 2014-72]
- Multiple unspecified memory-corruption vulnerabilities that exist in the browser engine. [CVE-2014-1553, CVE-2014-1554, MFSA 2014-67]
- A memory-corruption vulnerability that exists in the 'mozilla::DOMSVGLength::GetTearOff'. Specifically, this issue occurs due to a use-after-free error when interacting with the SVG content through the document object model (DOM) with animating SVG content. [CVE-2014-1563, MFSA 2014-68]
- A remote memory-corruption vulnerability exists because of an out-of-bounds read during the creation of an audio timeline in Web Audio. Specifically, this issue affects 'mozilla::dom::AudioEventTimeline' function. [CVE-2014-1565, MFSA 2014-70]

Successful exploitation of these vulnerabilities could result in 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.

## **RECOMMENDATIONS:**

The following actions should be taken:

- Apply appropriate patches provided by Mozilla 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 click links from unknown sources, or to click links without verifying the intended destination.

## **REFERENCES:**

### **Mozilla:**

<https://www.mozilla.org/security/announce/2014/mfsa2014-67.html>

<https://www.mozilla.org/security/announce/2014/mfsa2014-68.html>

<https://www.mozilla.org/security/announce/2014/mfsa2014-69.html>

<https://www.mozilla.org/security/announce/2014/mfsa2014-70.html>

<https://www.mozilla.org/security/announce/2014/mfsa2014-71.html>

<https://www.mozilla.org/security/announce/2014/mfsa2014-72.html>

**CVE:**

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1553>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1554>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1562>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1563>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1564>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1567>

**Security Focus:**

<http://www.securityfocus.com/bid/69519>

<http://www.securityfocus.com/bid/69520>

<http://www.securityfocus.com/bid/69523>

<http://www.securityfocus.com/bid/69524>

<http://www.securityfocus.com/bid/69525>

<http://www.securityfocus.com/bid/69526>