

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:

11/21/2012

SUBJECT:

Multiple Vulnerabilities in Mozilla Products Could Allow Remote Code Execution

OVERVIEW:

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.

SYSTEMS AFFECTED:

- Firefox versions prior to 17.0
- Firefox Extended Support Release (ESR) version prior to 10.0.11
- Thunderbird versions prior to 17.0
- Thunderbird Extended Support Release (ESR) version prior to 10.0.11
- SeaMonkey version prior to 2.14

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 Mozilla Firefox, Thunderbird, and SeaMonkey. The details of these vulnerabilities are as follows:

- Multiple memory-corruption vulnerabilities in the browser engine that could lead to arbitrary code execution. These issues affect Firefox, Thunderbird, and SeaMonkey. [MFSA 2012-91-CVE-2012-5842, CVE-2012-5843]
- A buffer overflow vulnerability occurs while rendering GIF format images. This issue affects Firefox, Thunderbird, and SeaMonkey.[MFSA 2012-92 - CVE-2012-4202]

- A cross-site scripting vulnerability occurs when the 'evalInSandbox()' function sets a 'location.href' location reference. This issue affects Firefox, Thunderbird, and SeaMonkey.[MFSA 2012-93 - CVE-2012-4201]
- A denial-of-service vulnerability occurs when the SVG text on a path is combined with the setting of CSS properties. This issue affects Firefox, Thunderbird, and SeaMonkey.[MFSA 2012-94 - CVE-2012-5836]
- A privilege-escalation vulnerability occurs when a 'javascript: URL' selected from the list of the Firefox 'new tab' page inherits the privileges of the privileged 'new tab' page. This issue affects Firefox. [MFSA 2012-95 - CVE-2012-4203]
- A memory-corruption vulnerability occurs in the 'str_unescape' string in the Javascript engine that could lead to arbitrary code execution. This issue affects Firefox, Thunderbird, and SeaMonkey.[MFSA 2012-96 - CVE-2012-4204]
- A cross-site request forgery vulnerability and an information leakage vulnerability occur when 'XMLHttpRequest' objects created within sandboxes have the system principal instead of the sandbox principal. This issue affects Firefox, Thunderbird, and SeaMonkey.[MFSA 2012-97 - CVE-2012-4205]
- A DLL hijacking vulnerability occurs that leads to arbitrary code execution from a privileged account. This issue affects Firefox. [MFSA 2012-98- CVE-2012-4206]
- A security-bypass vulnerability occurs because 'XrayWrappers' object exposes chrome-only properties even when not present in a chrome compartment. [MFSA 2012-99 - CVE-2012-4208]
- A cross-site scripting vulnerability occurs due to improper security filtering for cross-origin wrappers. [MFSA 2012-100 - CVE-2012-5841]
- A cross-site scripting vulnerability occurs due to improper character decoding in the HZ-GB-2312 charset. [MFSA 2012-101 - CVE-2012-4207]
- An arbitrary code execution vulnerability and a cross-site scripting vulnerability occur when the script entered into the Developer Toolbar runs with chrome privileges. This issue affects Firefox. [MFSA 2012-102 - CVE-2012-5837]
- A cross-site scripting vulnerability occurs when the location property is set to top and can be accessed by binary plugins through top.location with a frame. [MFSA 2012-103 - CVE-2012-4209]
- A CSS and HTML injection vulnerability occurs when a maliciously crafted stylesheet is inspected in the Style Inspector. This issue affects Firefox. [MFSA 2012-104 - CVE-2012-4210]
- Multiple buffer overflow and user-after free vulnerabilities occur that lead to remote code execution. [MFSA 2012-105 - CVE-2012-4214, CVE-2012-4215, CVE-2012-4216, CVE-2012-5829, CVE-2012-5839, CVE-2012-5840, CVE-2012-4212, CVE-2012-4213, CVE-2012-4217, CVE-2012-4218]
- Multiple buffer overflow and user-after free vulnerabilities occur that lead to remote code execution. [MFSA 2012-106 - CVE-2012-5830, CVE-2012-5833, CVE-2012-5835, CVE-2012-5838]

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.

RECOMMENDATIONS:

The following actions should be taken:

- Upgrade 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/2012/mfsa2012-91.html>
<http://www.mozilla.org/security/announce/2012/mfsa2012-92.html>
<http://www.mozilla.org/security/announce/2012/mfsa2012-93.html>
<http://www.mozilla.org/security/announce/2012/mfsa2012-94.html>
<http://www.mozilla.org/security/announce/2012/mfsa2012-95.html>
<http://www.mozilla.org/security/announce/2012/mfsa2012-96.html>
<http://www.mozilla.org/security/announce/2012/mfsa2012-97.html>
<http://www.mozilla.org/security/announce/2012/mfsa2012-98.html>
<http://www.mozilla.org/security/announce/2012/mfsa2012-99.html>
<http://www.mozilla.org/security/announce/2012/mfsa2012-100.html>
<http://www.mozilla.org/security/announce/2012/mfsa2012-101.html>
<http://www.mozilla.org/security/announce/2012/mfsa2012-102.html>
<http://www.mozilla.org/security/announce/2012/mfsa2012-103.html>
<http://www.mozilla.org/security/announce/2012/mfsa2012-104.html>
<http://www.mozilla.org/security/announce/2012/mfsa2012-105.html>
<http://www.mozilla.org/security/announce/2012/mfsa2012-106.html>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4201>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4202>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4203>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4204>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4205>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4206>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4207>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4208>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4209>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4210>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4211>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4212>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4213>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4214>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4215>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4216>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4217>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4218>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5829>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5830>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5833>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5835>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5836>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5837>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5838>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5839>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5840>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5841>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5842>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5843>

SecurityFocus:

<http://www.securityfocus.com/bid/56607>