

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:

7/21/2010

SUBJECT:

Multiple Vulnerabilities in Mozilla Products Could Allow Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in the Mozilla Firefox, Mozilla Thunderbird and Mozilla 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.

These vulnerabilities may be exploited if a user visits, or is redirected to, a web page or opens a malicious file specifically crafted to take advantage of these vulnerabilities. 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. Failed exploit attempts may result in a denial-of-service condition.

SYSTEMS AFFECTED:

Mozilla Firefox 3.5.0 - 3.5.10
Mozilla Firefox 3.6 - 3.6.4
Mozilla SeaMonkey 2.0 - 2.0.5
Mozilla Thunderbird 3.0 - 3.0.2
Mozilla Thunderbird 3.0.4 - 3.0.5

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, Mozilla Thunderbird, and Mozilla SeaMonkey. Details of these vulnerabilities are as follows:

Memory Safety Bugs (MFS2010-34)

Multiple memory safety bugs exist in the browser engine used by multiple Mozilla products. Most of these bugs have shown evidence of memory corruption, however, the vulnerabilities could allow for the ability to run arbitrary code.

DOM attribute cloning remote code execution vulnerability (MFS2010-35)

An error was reported in the DOM attribute cloning routine where an event attribute node can be deleted while another object still contains a reference to it. This reference could subsequently be accessed, potentially allowing code execution in memory.

Use-after-free error in NodeIterator (MFSA2010-36)

An error was reported in Mozilla's implementation of `NodeIterator`. An attacker could create a malicious `NodeFilter` which would detach nodes from the DOM tree while it was being traversed. The use of a detached and subsequently deleted node could result in code being executed in memory.

Plugin parameter EnsureCachedAttrParamArrays remote code execution vulnerability (MFSA2010-37)

An error was reported in the code used to store the names and values of plugin parameter elements. A malicious page could embed plugin content which would cause a buffer overflow that could potentially result in code execution.

Arbitrary code execution using SJOW and fast native function (MFSA2010-38)

A cross-domain security-bypass vulnerability exists for Firefox and Thunderbird which if exploited could allow for the execution of arbitrary code. This issue occurs because a content script can access content objects within the browser's chrome through 'SJOW'. Please note, Firefox 3.5 and other Mozilla products built from Gecko 1.9.1 are not affected by this issue.

nsCSSValue::Array index integer overflow (MFSA2010-39)

It has been reported that an array class used to store CSS values contains an integer overflow vulnerability. The integer value used in allocating the size of the array could overflow, resulting in too small a memory buffer being created. This could result in code being executed in attacker-controlled memory.

nsTreeSelection dangling pointer remote code execution vulnerability (MFSA2010-40)

An integer overflow vulnerability exists in the implementation of the XUL `<tree>` element's `selection` attribute. This vulnerability could be used by an attacker to call deleted memory and run arbitrary code on a victim's computer.

Remote code execution using malformed PNG image (MFSA2010-41)

A buffer overflow exists in the Mozilla graphics code which consumes image data processed by libpng. A malformed PNG file could be created which would cause libpng to incorrectly report the size of the image to downstream consumers. This could result in code being executed in attacker-controlled memory.

Cross-origin data disclosure via Web Workers and importScripts (MFSA2010-42)

A cross-domain information-disclosure issue has been reported which affects multiple Mozilla products. This issue affects the Web Worker method `'importScript()'` and will allow attackers to read and parse resources from other domains when the content is not valid JavaScript.

Same-origin bypass using canvas context (MFSA 2010-43)

A cross-domain information-disclosure vulnerability affects Firefox and Thunderbird. This issue affects the canvas element and can be used to read content from other sites.

Characters mapped to U+FFFD in 8 bit encodings cause subsequent characters to vanish (MFSA 2010-44)

A security-weakness in Firefox and Thunderbird exists due to the undefined positions within various 8-bit character encodings are mapped to the sequence U+FFFD. An attacker can exploit this issue in conjunction with other latent vulnerabilities to conduct cross-site scripting attacks.

Multiple location bar spoofing vulnerabilities (MFSA 2010-45)

Three spoofing vulnerabilities exist which allow attackers to spoof the location bar so that an insecure page may be viewed as a secured page. This could then lead to other attacks, such as remote code execution or information disclosure.

Cross-domain data theft using CSS (MFSA 2010-46)

A cross-domain security-bypass vulnerability exists in which attackers could gain access to content in another domain by injecting invalid CSS selectors into a target site and then retrieving the data using a JavaScript API.

Cross-origin data leakage from script filename in error messages (MFSA-2010-47)

A cross-domain information-disclosure vulnerability exists which may allow attackers to leak sensitive URL parameters across domains.

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 visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Remind users not to download or open files from un-trusted websites.

REFERENCES:

Mozilla:

<http://www.mozilla.org/security/announce/2010/mfsa2010-35.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-36.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-37.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-38.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-39.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-40.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-41.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-42.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-43.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-44.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-45.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-46.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-47.html>

Secunia:

<http://secunia.com/advisories/39925/>

VUPEN:

<http://www.vupen.com/english/advisories/2010/1859>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0654>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1205>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1206>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1207>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1208>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1209>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1210>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1211>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1212>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1213>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1214>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1215>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2751>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2752>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2753>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2754>