

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:

4/29/2011

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. These vulnerabilities may be exploited if a user visits, or is redirected to a web page or opens a malicious file that is specifically designed to take advantage of these vulnerabilities. Successful exploitation of these vulnerabilities will 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:

- Mozilla Firefox prior to 4.0.1
- Mozilla Firefox prior to 3.6.17
- Mozilla Firefox prior to 3.5.19
- Mozilla Sea Monkey prior to 2.0.14
- Mozilla Thunderbird prior to 3.1.0

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 Sea Monkey. Details of these vulnerabilities are as follows:

Miscellaneous memory safety hazards (MFSA 2011-12)

Multiple memory corruption vulnerabilities in Firefox, Thunderbird, and SeaMonkey will allow an attacker to execute remote code on the victim machine.

Multiple dangling pointer vulnerabilities (MFSA 2011-13)

Multiple dangling pointer issues affect mChannel, mObserverList, and nsTreeRange objects. These vulnerabilities can be exploited if an attacker can control the contents of deleted memory prior to its access; if successful, remote code execution may be possible. This issue affects Firefox and SeaMonkey. Please note that Firefox 4 is not affected by these issues.

Information stealing via form history (MFSA 2011-14)

A Java applet could be used to mimic interaction with form autocomplete controls and steal entries from the form history. This would allow an attacker to steal personal information from an unsuspecting user. This issue affects Firefox and SeaMonkey. Please note that Firefox 4 is not affected by this issue.

Escalation of privilege through Java Embedding Plug-in (MFSA 2011-15)

The Java Embedding Plug-in (JEP) shipped with Mac OS X versions of Firefox could be exploited to obtain elevated access to resources on a user's system. Please note that Firefox 4 is not affected by this issue.

Directory traversal in resource: protocol (MFSA 2011-16)

The resource: protocol may be exploited to allow directory traversal and the loading of content from non-permitted locations on the Windows Operating System. The impact of this vulnerability depends on whether certain files exist in predictable locations. For instance, if particular images exist, it may indicate that certain software is installed. This issue affects Firefox, Thunderbird, and SeaMonkey.

WebGL ES Vulnerabilities (MFSA 2011-17)

Two vulnerabilities exist in WebGL ES which is used by Firefox 4. An attacker may be able to leverage the way the WebGL ES libraries are compiled without Address Space Layout Randomization (ASLR) protection to execute remote code on a victim machine. This flaw only appears to affect versions of Firefox that are compiled on the Windows Operating System.

XSLT generate-id() function heap address leak (MFSA 2011-18)

The XSLT generate-id() function returns a string that reveals a specific valid address of an object on the memory heap. It is possible that this memory address could be used by an attacker to exploit different memory corruption vulnerabilities. This issue affects Firefox and SeaMonkey.

Exploitation may occur if a user visits or is redirected to a web page, or receives a specially crafted email, which is specifically crafted to take advantage of these vulnerabilities. When an unsuspecting user visits the malicious site or views the email, the exploit will be triggered, resulting in various unwanted actions being taken in the context of the targeted application.

Successful exploitation of the remote code execution vulnerabilities may 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 download or open files from untrusted websites.
- Remind users not to open e-mail attachments from unknown users or suspicious e-mails.
- 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/2011/mfsa2011-12.html>
<http://www.mozilla.org/security/announce/2011/mfsa2011-13.html>
<http://www.mozilla.org/security/announce/2011/mfsa2011-14.html>
<http://www.mozilla.org/security/announce/2011/mfsa2011-15.html>
<http://www.mozilla.org/security/announce/2011/mfsa2011-16.html>
<http://www.mozilla.org/security/announce/2011/mfsa2011-17.html>
<http://www.mozilla.org/security/announce/2011/mfsa2011-18.html>

Security Focus:

<http://www.securityfocus.com/bid/47635>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0065>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0066>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0067>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0068>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0069>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0070>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0071>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0072>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0073>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0074>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0075>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0076>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0077>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0078>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0079>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0080>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0081>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1202>