

State of Alaska State Security Office



State of Alaska Cyber Security & Critical Infrastructure Cyber Advisory

December 10, 2010

The following cyber advisory was issued by the State of Alaska and was 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.

ADVISORY NUMBER:

SA2010-088

DATE(S) ISSUED:

12/10/2010

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 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 3.5.0 – 3.5.17
- Mozilla Firefox 3.6 – 3.6.12
- Mozilla Sea Monkey 2.0.1 – 2.0.10
- Mozilla Thunderbird 3.0.1 – 3.0.10
- Mozilla Thunderbird 3.1.1 – 3.1.6

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**DESCRIPTION:**

Multiple vulnerabilities have been discovered in Mozilla Firefox, Mozilla Thunderbird, and Mozilla Sea Monkey. Details of these vulnerabilities are as follows:

Miscellaneous memory safety hazards (MFSA 2010-74)

Multiple memory-corruption vulnerabilities have been identified in the browser engine that could allow an attacker to execute arbitrary code.

Buffer overflow and memory corruption using document.write (MFSA 2010-75)

A vulnerability has been identified as a result of an excessively long string that is passed to 'document.write'.

Privilege-escalation vulnerability (MFSA 2010-76)

A privilege-escalation vulnerability issue exists in Firefox and Sea Monkey when the [about:blank](#) window is injected with an '<isindex>' element.

XUL tree memory corruption vulnerability (MFSA 2010-77)

A memory-corruption vulnerability affects XUL <tree> objects that has HTML '<div>' elements nested in a '<treechildren>' element. Attackers can exploit this issue to run arbitrary code on the affected system.

Multiple unspecified OS font vulnerabilities (MFSA 2010-78)

Mozilla has reported multiple unspecified vulnerabilities can occur when downloading different operating-system fonts.

Java security bypass issue (MFSA 2010-79)

A security bypass issue was found in the way Firefox and Sea Monkey loads Java LiveConnect scripts. Malicious web content could load a Java LiveConnect script in a way that would result in the plug-in object having elevated privileges, allowing it to execute Java code.

Use-after-free error in nsDOMAttribute (MFSA 2010-80)

A use-after-free error has been reported that affects the 'nsDOMAttribute' node.

JavaScript integer overflow vulnerability (MFSA 2010-81)

An integer-overflow vulnerability has been discovered in Mozilla products that affects JavaScript arrays which is due to an error in the 'NewIdArray()'. 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.

Remote code execution vulnerability in 'XMLHttpRequestSpy' module' (MFSa 2010-82)

Mozilla Products are prone to an arbitrary code execution vulnerability affecting the 'XMLHttpRequestSpy' module of the Firebug add-on. This vulnerability exists due to an incomplete fix for CVE-2010-0179. Successful exploitation may result in remote code execution.

Multiple XSS vulnerabilities affect Firefox character encodings (MFSa 2010-84)

Multiple cross-site scripting vulnerabilities were identified in Firefox 'x-mac-arabic', 'x-mac-farsi', and 'x-mac-hebrew' character encodings. Certain characters were converted to angle brackets when displayed. If successfully exploited, an attacker could execute malicious JavaScript code.

Successful exploitation of these 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:

We recommend the following actions be taken:

- Upgrade Mozilla products as needed immediately after appropriate testing.
- Remind users not to download or open files from un-trusted websites.
- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted 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/2010/mfsa2010-74.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-75.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-76.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-77.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-78.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-79.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-80.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-81.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-82.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-84.html>

Security Focus:

<http://www.securityfocus.com/bid/45322>
<http://www.securityfocus.com/bid/45324>
<http://www.securityfocus.com/bid/45326>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3766>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3767>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3768>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3769>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3770>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3771>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3772>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3773>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3775>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3776>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3777>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3778>