

State of Alaska State Security Office



State of Alaska Cyber Security & Critical Infrastructure Cyber Advisory

September 9, 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:

SA2010-066

DATE(S) ISSUED:

9/09/2010

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 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. Failed exploit attempts may result in a denial-of-service condition.

SYSTEMS AFFECTED:

- Mozilla Firefox 3.5.0 – 3.5.11
- Mozilla Firefox 3.6 – 3.6.8
- Mozilla SeaMonkey 2.0 – 2.0.6
- Mozilla Thunderbird 3.0 – 3.0.6
- Mozilla Thunderbird 3.1.1 – 3.1.2

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:

Miscellaneous memory safety hazards (MFSa 2010-49)

Multiple memory-corruption vulnerabilities affect the browser engine. These issues can be exploited to cause denial-of-service conditions; arbitrary code execution may also be possible.

Frameset integer overflow vulnerability (MFSa 2010-50)

An integer-overflow vulnerability affects implementation of the HTML frameset element. The code responsible for parsing the frameset columns used an 8-byte counter for the column numbers. An attacker can exploit this issue to execute arbitrary code.

Dangling pointer vulnerability using DOM plugin array (MFSa 2010-51)

A dangling-pointer issue arises in the implementation of 'navigator.plugins' in which the 'navigator' plugin object could retain a pointer to the plugins array even after it had been destroyed. An attacker can exploit this issue to execute arbitrary code.

Windows XP DLL loading vulnerability (MFSa 2010-52)

A DLL vulnerability exists because the applications search for the 'dwmapi.dll' Dynamic Link Library file in the current working directory. The issue can be exploited by placing both a specially crafted library file and a file that is associated with the vulnerable applications in an attacker-controlled location. Using the applications to open the associated file will cause the arbitrary library file to be executed.

Heap buffer overflow in nsTextFrameUtils::TransformText (MFSa 2010-53)

A heap-buffer overflow exists when transforming text runs. An attacker can exploit this issue to execute arbitrary code.

Multiple Dangling pointer vulnerabilities in nsTreeSelection (MFSa 2010-54 and MFSa 2010-56)

The first dangling-pointer vulnerability exists due to an incomplete fix for CVE-2010-2753. This pointer held by a XUL tree selection could be freed and then later reused resulting in an attacker execution arbitrary code.

The second vulnerability exists in the XUL <tree>'s content view. One of the content view's methods for accessing the internal structure of the tree could be manipulated into removing a node prior to accessing it, resulting in the accessing of deleted memory. An attacker can run arbitrary code if successful in controlling the contents of this deleted memory prior to its access. Failed exploit attempts will likely result in denial-of-service conditions.

XUL tree removal crash and remote code execution (MFSA 2010-55)

A vulnerability affects XUL <tree> objects that can be exploited to cause certain sections of deleted memory to be accessed. An attacker can exploit this issue to potentially execute arbitrary code; failed exploit attempts will likely cause denial-of-service conditions.

Crash and remote code execution in normalizeDocument (MFSA 2010-57)

An arbitrary code-execution vulnerability exists due to a logic flaw when normalizing a document. When the normalization code runs, a static count of the document's child nodes is used in the traversal. An attacker can create a page that would remove DOM nodes resulting in the execution of arbitrary code.

Crash on Mac using fuzzed font in data: URL (MFSA 2010-58)

A remote code execution vulnerability exists when handling specially crafted fonts on Mac systems. This vulnerability could presumably result in an attacker's arbitrary code being executed. Failed exploit attempts may result in denial-of-service conditions.

SJOW creates scope chains ending in outer object (MFSA 2010-59)

A privilege-escalation issue affects the wrapper class 'XPCSafeJSObjectWrapper (SJOW)' in Firefox and Thunderbird. This wrapper class allows content-defined objects to be safely accessed by privileged code. Users of SJOWs may be given a chrome privileged object which could be leveraged to run arbitrary JavaScript with chrome privileges.

XSS using SJOW scripted function (MFSA 2010-60)

A same-origin-bypass issue affects the wrapper class 'XPCSafeJSObjectWrapper (SJOW)'. This wrapper class allows the caller to run the function within the context of another site. This issue could allow an attacker to execute a XSS (cross-site scripting) attack.

UTF-7 XSS by overriding document charset using <object> type attribute (MFSA 2010-61)

A cross-site scripting issue exists when handling the 'type' attribute of an <object> tag. An attacker can construct a page containing this <object> tag which sets the charset to UTF-7 allowing them to encode JavaScript in order to bypass the site's XSS filters.

Copy-and-paste or drag-and-drop into designMode document allows XSS(MFSA 2010-62)

A cross-site scripting issue exists when handling a document and having 'designMode' enabled. When an HTML selection containing JavaScript is copy-and-pasted or dropped onto a document with designMode enabled the JavaScript will be executed within the context of the site where the code was dropped. An attacker can leverage this issue to execute a XSS (cross-site scripting) attack.

Information leak via XMLHttpRequest status Text (MFSA 2010-63)

An information-disclosure exists in the 'statusText' property of an XMLHttpRequest object. This issue can disclose the presence of a web server and to gather information about servers on internal networks.

RECOMMENDATIONS:

We recommend the following actions 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/mfsa2010-49.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-50.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-51.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-52.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-53.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-54.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-55.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-56.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-57.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-58.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-59.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-60.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-61.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-62.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-63.html>

Secunia:

<http://secunia.com/advisories/41297>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3166>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3167>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3168>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3169>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2760>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2762>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2763>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2764>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2765>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2766>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2767>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2768>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2769>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2770>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3131>