



State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory

March 31, 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:

SA2010-023

DATE(S) ISSUED:

3/31/2010

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 webpage 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 version 3.6
- Mozilla Firefox version 3.5.8 and earlier
- Mozilla Firefox version 3.0.18 and earlier
- Mozilla SeaMonkey 2.0.3 and earlier
- Mozilla Thunderbird 3.0.2 and earlier

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:

Mozilla Firefox, Thunderbird and SeaMonkey Multiple Vulnerabilities May Cause Remote Code Execution (MFSA2010-16)

Mozilla Products are prone to memory corruption vulnerabilities affecting the browser engine that can cause a denial of service. Remote code execution may also be possible but has not been confirmed.

Mozilla Firefox, Thunderbird and SeaMonkey Vulnerability May Cause Remote Code Execution with Use-After-Free in nsTreeSelection (MFSA2010-17)

Mozilla Products are prone to a remote code execution vulnerability because the 'use-after-free' event handler in 'nsTreeSelection' can be called after the XUL tree item is deleted, resulting in the execution of previously freed memory.

Mozilla Firefox, Thunderbird, and SeaMonkey Dangling Pointer Vulnerability in nsTreeContentView (MFSA2010-18)

Mozilla Products are prone to a dangling-pointer vulnerability in 'nsTreeContentView'.. The vulnerability occurs due a flaw when '<option>' elements are inserted into an '<optgroup>' XUL tree, that can result in an under-counted number of element references during element deletion.

Mozilla Firefox and SeaMonkey Dangling Pointer Vulnerability in nsPluginArray (MFSA2010-19)

Mozilla Products are prone to a dangling-pointer vulnerability in 'nsPluginArray' due to a flaw in the implementation of the 'window.navigator.plugins' object.. After a page is reloaded, the 'nsPluginsArray' fails to check for existing member references prior to reallocating its members. This can cause objects with existing pointers to be deleted while leaving the pointer intact.

Mozilla Firefox and SeaMonkey Chrome Privilege Escalation via Forced URL Drag and Drop (MFSA2010-20)

Mozilla Products are prone to a privilege escalation vulnerability due to a forced URL drag and drop. Attackers can leverage this issue to execute arbitrary script code with chrome privileges.

Mozilla Firefox and SeaMonkey Arbitrary Code Execution with Firebug XMLHttpRequestSpy (MFSA2010-21)

Mozilla Products are prone to an arbitrary code execution vulnerability affecting the 'XMLHttpRequestSpy' module of the Firebug add-on. This issue occurs because the 'XMLHttpRequestSpy' object fails to properly wrap various property attachments defined in web content. Attackers can exploit this issue to execute arbitrary script code with escalated privileges.

Mozilla Firefox, Thunderbird, SeaMonkey Update NSS to Support TLS Renegotiation Indication (MFSA2010-22)

Mozilla Products have added support in the Network Security Services module for preventing a type of man-in-the-middle attack against TLS using forced renegotiation.

Mozilla Firefox and SeaMonkey Image src Redirect to mailto: URL Opens Email Editor (MFSA2010-23)

When an image tag points to a resource that redirects to a mailto: URL, the external mail handler application is launched. This issue poses no security threat to users but could create an annoyance when browsing a site that allows users to post arbitrary images.

Mozilla Firefox, Thunderbird, SeaMonkey XMLHttpRequest::load() Doesn't Check nsIContentPolicy (MFSA2010-24)

Mozilla Products fail to call certain security checks when loading new content from XML documents. This could result in certain resources being loaded that would otherwise violate security policies set by the browser or installed add-ons.

The above vulnerabilities may be exploited if a user visits or is redirected to a webpage 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.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Upgrade to Mozilla Firefox version 3.6.2 or 3.5.9 or 3.0.19, Thunderbird 3.0.4, and SeaMonkey 2.0.4 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/mfsa2010-16.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-17.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-18.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-19.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-20.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-21.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-22.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-23.html>
<http://www.mozilla.org/security/announce/2010/mfsa2010-24.html>

Vupen:

<http://www.vupen.com/english/advisories/2010/0748>

Secunia:

<http://secunia.com/advisories/39240/>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3555>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0173>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0174>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0175>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0176>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0177>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0178>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0179>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0181>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0182>