



**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory**

December 20, 2011

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:

SA2011-074

DATE(S) ISSUED:

12/20/2011

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 specially crafted web page. Successful exploitation of these vulnerabilities could result in either an attacker gaining the same privileges as the logged on user. 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:

Firefox 8.0
Firefox 8.0.1
Thunderbird 8.0
SeaMonkey 2.5

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, Thunderbird, and SeaMonkey. The details of these vulnerabilities are as follows:

Several unspecified memory safety vulnerabilities have been discovered in Firefox, Thunderbird, and SeaMonkey. Some of these vulnerabilities show evidence of memory corruption under certain circumstances, and could be exploited to run arbitrary code. These vulnerabilities can be exploited if a user visits a specially crafted webpage or views a specially crafted email with scriptingenabled. (CVE-2011-3660)

An unspecified vulnerability exists in the YARR regular expression library in Firefox. This vulnerability can be exploited if a user visits a website that contains a specially crafted java script. Successful exploitation could lead to remote code execution. (CVE-2011-3661)

A vulnerability exists in the Mozilla Firefox, SeaMonkey, and Thunderbird SVGimplementation that could result in out-of-bounds memory access. Thunderbird and SeaMonkey are vulnerable if they are configured to allow scripting. This issue exists due to the way SVG elements are removed during a DOMAttrModified event handler. This vulnerability can be exploited if a user visits a specially crafted webpage. Successful exploitation could lead to remote code execution. (CVE-2011-3658)

A vulnerability exists in Mozilla SVG animation accessKey events that allows key strokes to be captures when scripting is disabled. This vulnerability can be exploited when a user visits a specially crafted webpage. The attacker could then capture keystrokes without the user submitting information to the server. (CVE-2011-3663)

An unspecified vulnerability exists in Mozilla products when a plug-in deletes its DOM frame during a call from that frame. In Firefox, this vulnerability can be exploited if a user visits a specially crafted webpage. Successful exploitation could lead to data exfiltration or malicious actions being performed by theuser on behalf of the attacker. (CVE-2011-3664)

An unspecified vulnerability exists in Mozilla products when scaling an OGG<video> element to extreme sizes. Successful exploitation could lead to remote code execution. The details of how this vulnerability can be exploited are unavailable. (CVE-2011-3665)

A vulnerability exists in Mozilla Firefox and Mozilla Thunderbird due to the improper handling of .jar files. This issue exists due to an incomplete patch for Firefox and Thunderbird on MacOSX. (CVE-2011-3666)

Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. 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:

- Install the appropriate vendor patch as soon as it becomes available after appropriate testing.

- Remind users not to visit un-trusted websites or follow links provided by unknown or un-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/2011/mfsa2011-53.html>
<http://www.mozilla.org/security/announce/2011/mfsa2011-54.html>
<http://www.mozilla.org/security/announce/2011/mfsa2011-55.html>
<http://www.mozilla.org/security/announce/2011/mfsa2011-56.html>
<http://www.mozilla.org/security/announce/2011/mfsa2011-57.html>
<http://www.mozilla.org/security/announce/2011/mfsa2011-58.html>
<http://www.mozilla.org/security/announce/2011/mfsa2011-59.html>

CVE

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3660>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3661>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3658>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3663>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3664>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3665>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3666>

Security Focus

<http://www.securityfocus.com/bid/51138>
<http://www.securityfocus.com/bid/51135>
<http://www.securityfocus.com/bid/51136>
<http://www.securityfocus.com/bid/51133>
<http://www.securityfocus.com/bid/51133>
<http://www.securityfocus.com/bid/51139>