



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

June 6, 2012

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.

MS-ISAC ADVISORY NUMBER:

SA2012-032

DATE(S) ISSUED:

6/5/2012

6/6/2012 - UPDATED

SUBJECT:

Multiple Vulnerabilities in Mozilla Products Could Allow Remote Code Execution

ORIGINAL 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. 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.

SYSTEMS AFFECTED:

- Firefox versions prior to 13.0
- Thunderbird versions prior to 13.0
- SeaMonkey versions prior to 2.10

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:

Heap Buffer Overflow Vulnerability

A heap based buffer overflow vulnerability has been discovered which can be triggered when converting from Unicode to native character sets using the function 'utf16_to_osilatin1'. Successful exploitation could result in remote code execution. Failed attacks may result in a denial of service condition. (CVE-2012-1947)

Heap Buffer Overflow Vulnerability

A heap based buffer overflow vulnerability has been discovered in 'nsHTMLReflowState::CalculateHypotheticalBox' which occurs when a window is resized on a page with nested columns. Successful exploitation could result in remote code execution. Failed attacks may result in a denial of service condition. (CVE-2012-1941)

These vulnerabilities may be exploited if a user visits a maliciously crafted web page. The page will consist of excessive data, memory addresses, machine code, and possibly NOP instructions. Successful exploitation could result in an attacker executing arbitrary code in the context of the user running the affected application. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

June 6 - UPDATED DESCRIPTION:

Mozilla has issued MFSA 2012-34 which details additional vulnerabilities which are mitigated by the latest updates. The details of these vulnerabilities are as follows:

Memory Corruption Vulnerability

A remote memory corruption vulnerability has been discovered related to 'methodjit/ImmutableSync.cpp', the 'JSObject::makeDenseArraySlow' function in js/src/jsarray.cpp, and other unknown components. Successful exploitation could result in remote code execution. Failed attacks may result in a denial of service condition. (CVE-2012-1938)

Memory Corruption Vulnerability

A remote memory corruption vulnerability has been discovered related to an assertion failure in 'jsinfer.cpp' which could allow attackers to execute code. Successful exploitation could result in remote code execution. Failed attacks may result in a denial of service condition. Note that this issue only affects Mozilla Firefox ESR 10.x before 10.0.5 and Thunderbird ESR 10.x before 10.0.5. (CVE-2012-1939)

Memory Corruption Vulnerability

An unspecified remote memory corruption vulnerability has been discovered which could allow attackers to execute code via unknown vectors. Failed attacks may result in a denial of service condition. (CVE-2012-1937)

RECOMMENDATIONS:

We recommend the following actions be taken:

- Upgrade vulnerable Mozilla products immediately after appropriate testing.

- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Do not open email attachments or click on URLs from unknown or untrusted 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/2012/mfsa2012-40.html>

SecurityFocus:

<http://www.securityfocus.com/bid/53791>

<http://www.securityfocus.com/bid/53793>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1947>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1941>

June 6 - UPDATED REFERENCES:

Mozilla:

<http://www.mozilla.org/security/announce/2012/mfsa2012-34.html>

SecurityFocus:

<http://www.securityfocus.com/bid/53796>

<http://www.securityfocus.com/bid/53797>

<http://www.securityfocus.com/bid/53800>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1938>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1939>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1937>