

State of Alaska State Security Office



State of Alaska Cyber Security & Critical Infrastructure Cyber Advisory

June 23, 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:

SA2010-044

DATE(S) ISSUED:

6/23/2010

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 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 3.5.9 and earlier
- Mozilla Firefox 3.6.3 and earlier
- Mozilla SeaMonkey 2.0.4 and earlier
- Mozilla Thunderbird 3.0.4 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:

Eight vulnerabilities have been discovered in Mozilla Firefox, Mozilla Thunderbird and Mozilla SeaMonkey. Details of these vulnerabilities are as follows:

Multiple memory corruption vulnerabilities (MFSA2010-26)

Multiple memory corruption vulnerabilities affecting the browser and JavaScript engine can allow remote attackers to crash the browser or execute arbitrary code in the context of the application. 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.

A use-after-free error can allow for the execution of arbitrary code (MFSA2010-27)

A use-after-free error affects the 'nsCycleCollector::MarkRoots()' function, which can allow attackers to execute arbitrary code. 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.

Multiple plugin instances may share references resulting in arbitrary code execution (MFSA2010-28)

Multiple plugin instances may share references, which may result in the execution of arbitrary code. 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.

A heap-based buffer-overflow may result in the execution of arbitrary code (MFSA2010-29)

A heap-based buffer-overflow issue affects the 'nsGenericDOMDataNode::SetTextInternal()' function. The issue can be triggered when overly long strings are used to set the text value for certain DOM nodes. Attackers can exploit this issue to run arbitrary code. 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.

An integer-overflow issue may result in the execution of arbitrary code (MFSA2010-30)

An integer-overflow issue affects XSLT node sorting. Attackers can exploit this issue to run arbitrary code. 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.

focus() behavior can be used to inject or steal keystrokes (MFSa2010-31)

A vulnerability issue with the focus() behavior can be used by an attacker to inject or steal keystrokes. This issue could result in an attacker changing a user's cursor focus while they are typing and potentially allow the attacker to gain sensitive information such as passwords.

A security-bypass issue may allow for cross site scripting (MFSa2010-32)

A security-bypass issue affects attachments with 'Content-Disposition' HTTP headers. The header is ignored when 'Content-Type: multipart' headers are also present. Attackers can leverage this issue to create cross-site scripting attacks on certain web pages that may allow users to upload arbitrary files.

User tracking across sites using Math.random() (MFSa2010-33)

A vulnerability issue in Math.random() can be used to identify and track users across different web sites. This could aid attackers in certain phishing attack scenarios.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Upgrade to Mozilla Firefox version 3.6.4 or 3.5.10, Thunderbird 3.0.5, or SeaMonkey 2.0.5 as needed 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 web sites or follow links provided by unknown or un-trusted sources.
- Remind users not to download or open files from un-trusted web sites.

REFERENCES:**Security Focus:**

<http://www.securityfocus.com/bid/41050>

Mozilla Foundation:

<http://www.mozilla.org/security/announce/2010/mfsa2010-26.html>

<http://www.mozilla.org/security/announce/2010/mfsa2010-27.html>

<http://www.mozilla.org/security/announce/2010/mfsa2010-28.html>

<http://www.mozilla.org/security/announce/2010/mfsa2010-29.html>

<http://www.mozilla.org/security/announce/2010/mfsa2010-30.html>

<http://www.mozilla.org/security/announce/2010/mfsa2010-31.html>

<http://www.mozilla.org/security/announce/2010/mfsa2010-32.html>

<http://www.mozilla.org/security/announce/2010/mfsa2010-33.html>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5913>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0183>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1125>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1196>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1197>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1198>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1199>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1200>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1201>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1202>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1203>

