

State of Alaska State Security Office



State of Alaska Cyber Security & Critical Infrastructure Cyber Advisory

October 20, 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:
SA2010-079

DATE(S) ISSUED:
10/20/2010

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 that is specifically designed 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 – 3.5.12
- Mozilla Firefox 3.6 – 3.6.10
- Mozilla Sea Monkey 2.0 – 2.0.7
- Mozilla Thunderbird 3.0 – 3.0.7
- Mozilla Thunderbird 3.1.1 – 3.1.4

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 2010-64)

Multiple memory-corruption vulnerabilities have been identified in the browser engine.

Buffer overflow and memory corruption using document.write (MFSA 2010-65)

A vulnerability has been identified as a result of an excessively long string that is passed to 'document.write'.

Use-after-free error in nsBarProp (MFSA 2010-66)

A use-after-free error affects the 'locationbar' property of a closed window object.

Dangling pointer vulnerability in LookupGetterOrSetter (MFSA 2010-67)

A dangling pointer issue affects the 'LookupGetterOrSetter()' function of 'js3250.dll' when

called with no arguments

XSS in gopher parser when parsing hrefs (MFSA 2010-68)

A cross-site scripting vulnerability has been identified in Mozilla Firefox and SeaMonkey in the Gopher parser when processing 'hrefs'.

Cross-site information disclosure via modal calls (MFSA 2010-69)

A cross-domain information disclosure vulnerability has been reported that affects multiple Mozilla products which affects 'modal' calls.

SSL wildcard certificate matching IP addresses (MFSA 2010-70)

It has been reported that if an SSL certificate is created with a common name containing a wildcard followed by a partial IP address that a valid SSL connection could be established with a server whose IP address matched the wildcard range.

Unsafe library loading vulnerabilities (MFSA 2010-71)

Multiple Mozilla products have been reported as unsafely loading external libraries from the current working directory. An attacker can take advantage of this vulnerability by placing a malicious DLL in the current working directory

Insecure Diffie-Hellman key exchange (MFSA 2010-72)

A vulnerability has been identified in the SSL implementation when using the Diffie-Hellman Ephemeral mode (DHE).

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.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Upgrade Mozilla products as needed immediately after appropriate testing.
- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from un-trusted sources.

- 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.

REFERENCES:

Mozilla:

<http://www.mozilla.org/security/announce/2010/mfsa2010-64.html>

<http://www.mozilla.org/security/announce/2010/mfsa2010-65.html>

<http://www.mozilla.org/security/announce/2010/mfsa2010-66.html>

<http://www.mozilla.org/security/announce/2010/mfsa2010-67.html>

<http://www.mozilla.org/security/announce/2010/mfsa2010-68.html>

<http://www.mozilla.org/security/announce/2010/mfsa2010-69.html>

<http://www.mozilla.org/security/announce/2010/mfsa2010-70.html>

<http://www.mozilla.org/security/announce/2010/mfsa2010-71.html>

<http://www.mozilla.org/security/announce/2010/mfsa2010-72.html>

Security Focus:

<http://www.securityfocus.com/bid/44228>

<http://www.securityfocus.com/bid/44243>

<http://www.securityfocus.com/bid/44245>

<http://www.securityfocus.com/bid/44246>

<http://www.securityfocus.com/bid/44247>

<http://www.securityfocus.com/bid/44248>

<http://www.securityfocus.com/bid/44249>

<http://www.securityfocus.com/bid/44250>

<http://www.securityfocus.com/bid/44251>

<http://www.securityfocus.com/bid/44252>

<http://www.securityfocus.com/bid/44253>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3170>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3173>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3174>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3175>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3176>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3177>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3178>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3179>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3180>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3181>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3182>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3183>