



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

April 24, 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.

ADVISORY NUMBER:

SA2012-023

DATE(S) ISSUED:

4/24/2012

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. 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 12.0
- Firefox Mobile versions prior to 10.0.4
- Thunderbird versions prior to 12.0
- SeaMonkey versions prior to 2.9

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:

Miscellaneous Memory Safety Hazards (MFSA2012-20)

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. (CVE-2012-0467)

Multiple Security Flaws in FreeType v2.4.9 (MFSA2012-21)

A series of unspecified memory safety bugs in the FreeType library for Firefox Mobile versions prior to 10.0.4 have been discovered. Successful exploitation could result in remote code execution. (CVE-2012-1126 – CVE-2012-1144)

IDBKeyRange Use After Free (MFSA2012-22)

A vulnerability exists in Mozilla products due to the improper handling of 'IDBKeyRange'. Successful exploitation could result in remote code execution. (CVE-2012-0469)

Invalid Frees Causes Heap Corruption in "gfxImageSurface" (MFSA2012-23)

A heap corruption vulnerability exists in 'gfxImageSurface' which allows for invalid frees and possible remote code execution. This occurs due to a float error resulting from graphics values being passed through different number systems. Successful exploitation could result in remote code execution. (CVE-2012-0470)

Cross-Site Scripting via Multi-Byte Content Processing Errors (MFSA2012-24)

A multi-octet encoding issue exists in Mozilla products where certain octets will destroy the following octets in the processing of some multi-byte character sets. This could leave users vulnerable to cross-site scripting attacks on specially crafted web pages. (CVE-2012-0471)

Memory Corruption During Font Rendering (MFSA2012-25)

A memory corruption vulnerability exists on Mozilla products installed on Windows Vista and Windows 7 systems with hardware acceleration disabled or using incompatible video drivers. This vulnerability exists due to 'cairo-dwrite' attempting to render fonts on an unsupported code path. Successful exploitation could result in remote code execution. (CVE-2012-0472)

WebGL.drawElements May Read Illegal Video Memory (MFSA2012-26)

A vulnerability exists in the 'FindMaxElementInSubArray' due to the reception of improper arguments from 'FindMaxUshortElement'. This issue causes maximum index to be computed incorrectly within 'WebGL.drawElements', allowing the reading of illegal video memory. Successful exploitation could allow information disclosure or code injection. (CVE-2012-0473)

Page Load Short-Circuit can Lead to Cross-Site Scripting (MFSA2012-27)

A vulnerability exists in Mozilla products that could cause web page loads to show the address of a different site than what is loaded in the window in the address bar. Successful exploitation could result in cross-site scripting attacks. (CVE-2012-0474)

Ambiguous IPv6 in Origin Headers May Bypass Web Server Access Restrictions (MFSA2012-28)

A security bypass vulnerability exists in Mozilla products when a web server opens a socket on a non-standard port for web traffic while using an IPv6 address. The browser will send ambiguous origin headers if the IPv6 address contains at least two consecutive 16-bit fields of zeroes. If there is an origin access control list that uses IPv6 literals, this issue could be used to bypass these access controls on the server. (CVE-2012-0475)

Potential Cross-Site Scripting Through Decoding Issues (MFSA2012-29)

A vulnerability exists in Mozilla products during the decoding of ISO-2022-KR and ISO-2022-CN character sets. Characters near 1024 bytes are treated incorrectly. On certain web pages it might be possible for an attacker to pad the output of the page such that these errors fall in the right place to affect the structure of the page, allowing for cross-site scripting. (CVE-2012-0477)

Crash with WebGL Content Using 'texImage2D' (MFSA2012-30)

An image rendering issue exists in Mozilla products 'WebGL' when 'texImage2D' uses 'JSVAL_TO_OBJECT' on arbitrary objects. This can lead to a crash on a specially crafted web page potentially resulting in remote code execution. (CVE-2012-0478)

Off-by-one Error in OpenType Sanitizer (MFSA2012-31)

An off-by-one error exists in the OpenType Sanitizer using the Address Sanitizer tool. This can lead to an out-of-bounds read and execution of an uninitialized function pointer during parsing resulting in possible remote code execution. (CVE-2011-3062)

HTTP Redirection and Remote Content Javascript Read Errors (MFSA2012-32)

A unspecified defect in the error handling of Javascript errors can leak the file names and location of Javascript files on a server, leading to inadvertent information disclosure and a vector for further attacks. (CVE-2011-1187)

Potential Site Identity Spoofing When Loading RSS and Atom feeds (MFSA2012-33)

A vulnerability exists in Mozilla products if specially crafted RSS or Atom XML content is loaded over HTTPS. The address bar updates to display the new location of the loaded resource, including SSL indicators, while the main window still displays the previously loaded content. This allows for phishing attacks where a malicious page can spoof the identify of another seemingly secure site. (CVE-2012-0479)

These vulnerabilities may be exploited if a user visits a maliciously crafted web page. Successful exploitation could result in an attacker gaining user level privileges. 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.

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/mfsa2012-20.html>
<http://www.mozilla.org/security/announce/2012/mfsa2012-21.html>
<http://www.mozilla.org/security/announce/2012/mfsa2012-22.html>
<http://www.mozilla.org/security/announce/2012/mfsa2012-23.html>
<http://www.mozilla.org/security/announce/2012/mfsa2012-24.html>
<http://www.mozilla.org/security/announce/2012/mfsa2012-25.html>
<http://www.mozilla.org/security/announce/2012/mfsa2012-26.html>
<http://www.mozilla.org/security/announce/2012/mfsa2012-27.html>
<http://www.mozilla.org/security/announce/2012/mfsa2012-28.html>
<http://www.mozilla.org/security/announce/2012/mfsa2012-29.html>
<http://www.mozilla.org/security/announce/2012/mfsa2012-30.html>
<http://www.mozilla.org/security/announce/2012/mfsa2012-31.html>
<http://www.mozilla.org/security/announce/2012/mfsa2012-32.html>
<http://www.mozilla.org/security/announce/2012/mfsa2012-33.html>

SecurityFocus:

<http://www.securityfocus.com/bid/53223>
<http://www.securityfocus.com/bid/52318>
<http://www.securityfocus.com/bid/53220>
<http://www.securityfocus.com/bid/53225>
<http://www.securityfocus.com/bid/53219>
<http://www.securityfocus.com/bid/53218>
<http://www.securityfocus.com/bid/53228>
<http://www.securityfocus.com/bid/53229>
<http://www.securityfocus.com/bid/53227>
<http://www.securityfocus.com/bid/53222>
<http://www.securityfocus.com/bid/53224>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0467>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1126>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1127>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1128>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1129>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1130>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1131>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1132>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1133>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1134>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1135>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1136>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1137>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1138>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1139>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1140>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1141>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1142>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1143>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1144>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0469>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0470>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0471>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0472>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0473>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0474>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0475>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0477>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0478>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3062>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1187>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0479>