

ISSO Information Alert

2/1/2012

Mozilla Vulnerabilities Could Allow Remote Code Execution

MULTI-STATE INFORMATION SHARING AND ANALYSIS CENTER CYBER SECURITY ADVISORY

MS-ISAC ADVISORY NUMBER:

2012-005

DATE(S) ISSUED:

2/1/2012

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 9.0.1
- Thunderbird versions prior to 9.0
- SeaMonkey versions prior to 2.6

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

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.

Overly permissive IPv6 literal syntax

Requests made using IPv6 syntax using XMLHttpRequest objects through a proxy may generate errors depending on proxy configuration for IPv6. The resulting error messages from the proxy may disclose sensitive data because Same-Origin Policy (SOP) will allow the XMLHttpRequest object to read these error messages, allowing user privacy to be eroded.

Cross Domain Security Bypass Vulnerability

An attacker could replace a sub-frame in another domain's document by using the name attribute of the sub-frame as a form submission target. This can potentially allow for phishing attacks against users and violates the HTML5frame navigation policy.

Use After Free Memory Corruption Vulnerability

A use-after-free memory-corruption vulnerability occurs because the removed child nodes of 'nsDOMAttribute' can be accessed under certain circumstances due to premature notification of 'AttributeChildRemove()'. This vulnerability could be exploited to possibly allow for remote code execution.

Cross Domain Scripting Vulnerability

A CrossDomain Scripting Vulnerability can occur when the application allows attackers to bypass the XPCConnect security check when calling an untrusted object. This occurs if an attacker replaces a sub-frame in another domain's document by using the name attribute of a sub-frame as an HTML form submission target

Information Disclosure Vulnerability

An Information Disclosed vulnerability occurs due to the appending of uninitialized memory to the encoded PNG images when converted from an ICO image format (image/vnd.microsoft.icon). As a result, sensitive data may be disclosed in the resulting image.

Memory Corruption Vulnerability

A memory corruption vulnerability can occur when decoding specially crafted Ogg Vorbis files (media file format). When exploited, this could result in a crash during the debug process and has the potential of remote code execution.

Denial of Service Vulnerability

A Denial of Service vulnerability can occur due to memory corruption when processing a malformed embedded XSLT stylesheet. Per Mozilla, there is no evidence that this vulnerability is directly exploitable. However, there is a possibility of remote code execution.

Firefox Recovery Key.html is saved with unsafe permission

If a user chooses to export their Firefox Sync key and the "Firefox Recovery Key.html" file is saved with incorrect permissions, this could result in making the file readable by other users on Linux and OS X based systems.

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/mfsa2012-01.html>

<http://www.mozilla.org/security/announce/2012/mfsa2012-02.html>

<http://www.mozilla.org/security/announce/2012/mfsa2012-03.html>

<http://www.mozilla.org/security/announce/2012/mfsa2012-04.html>

<http://www.mozilla.org/security/announce/2012/mfsa2012-05.html>

<http://www.mozilla.org/security/announce/2012/mfsa2012-06.html>

<http://www.mozilla.org/security/announce/2012/mfsa2012-07.html>

<http://www.mozilla.org/security/announce/2012/mfsa2012-08.html>

<http://www.mozilla.org/security/announce/2012/mfsa2012-09.html>

SecurityFocus:

<http://www.securityfocus.com/bid/51752>

<http://www.securityfocus.com/bid/51753>

<http://www.securityfocus.com/bid/51754>

<http://www.securityfocus.com/bid/51755>

<http://www.securityfocus.com/bid/51756>

<http://www.securityfocus.com/bid/51757>

<http://www.securityfocus.com/bid/51765>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0444>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0443>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3659>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0447>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0446>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0445>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0449>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0450>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3670>