

*The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is 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.*

**DATE(S) ISSUED:**

08/17/2011

**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. These vulnerabilities may be exploited if a user visits, or is redirected to a specially crafted web page. 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.

**SYSTEMS AFFECTED:**

- Mozilla Firefox prior to 3.6.20
- Mozilla Firefox prior to 6.0
- Mozilla Sea Monkey prior to 2.4
- Mozilla Thunderbird prior to 3.1.12
- Mozilla Thunderbird prior to 6.0

**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 Sea Monkey. Details of these vulnerabilities are as follows:

- A memory corruption vulnerability has been discovered in the WebGL (Web-based Graphics Library) component of Mozilla products. WebGL is used to expand the capabilities of JavaScript to allow the generation of 3D graphics on supported browsers. It is currently in use on multiple Mozilla products and enabled by default in Firefox. This issue affects Firefox 4 and 5, and Thunderbird 5 (CVE-2011-2989)
- Memory corruption vulnerabilities have been discovered in the JavaScript engine, this affects Firefox 4 and 5; Thunderbird 5, and SeaMonkey 2.2. (CVE-2011-2991)

- Memory corruption vulnerabilities have been discovered in the Ogg reader found in many Mozilla products. Ogg is an open source file format used for streaming and manipulation of digital multimedia. This issue affects Firefox 4 and 5; and Thunderbird 5. (CVE-2011-2992)
- Multiple unspecified memory corruption vulnerabilities have been discovered affecting Firefox 4 and 5; and Thunderbird 5. (CVE-2011-2985)
- Multiple unspecified memory corruption vulnerabilities affect Firefox 3.6 (CVE-2011-2982)
- A security bypass issue has been found that affects multiple Mozilla applications. If exploited it could allow attackers to call a script available inside a signed Java Archive (JAR) from an unsigned JavaScript. Successful exploitation could result in an attacker's specially crafted site(s) inheriting the privileges of the signed JAR file. This issue affects the Firefox 4 and 5; and SeaMonkey 2.2. (CVE-2011-2993)
- A buffer overflow vulnerability was discovered in various Mozilla applications, which occurs when processing an overly long WebGL shader program. (CVE-2011-2988)
- A heap overflow issue affects the ANGLE library, which is used in the implementation of WebGL to render 3D images. Successful exploitation could result in data corruption, denial of service, or remote code execution. This issue affects Firefox 4 and 5; and SeaMonkey 2.2. (CVE-2011-2987)
- A memory corruption vulnerability affects the Scalable Vector Graphics (SVG) text manipulation routine due to a dangling pointer error, which occurs in the SVGTextElement.getCharNumAtPosition()' function. An HTML mail message containing a malicious SVG image could cause Mozilla products to crash or, potentially, execute arbitrary code with the privileges of the user running applications. This issue affects Firefox 3.6.19, 4 and 5; and Thunderbird 3.1.11 and 5; and SeaMonkey 2.2. (CVE-2011-0084)
- An information disclosure vulnerability occurs because Content Security Policy violation reports fail to strip out proxy authorization credentials from the list of request headers. This could cause a website with Content Security Policy enabled to incorrectly resolve the constructed host policy. This affects Firefox 6.0. (CVE-2011-2990)
- An information disclosure vulnerability occurs because of a cross-origin issue when using canvas and Windows Direct 2D hardware acceleration. Image data from one web server could be inserted into a canvas and read by a different web server. This affects Firefox 6.0 (CVE-2011-2986)
- A Privilege escalation issue occurs when using event handlers, which allows JavaScript to run in the context of a different website or in a chrome-privileged context. This affects Firefox 3.6.20 and 3.1.12 (CVE-2011-2981)
- A memory corruption issue affects the 'appendChild()' function because of a dangling pointer error. This affects Firefox 3.6.20 and 3.1.12 (CVE-2011-2378)
- A Privilege escalation issue occurs when dropping a tab element in a content area, which allows web content to run in a chrome privileged context. This affects Firefox 3.6.20 and 3.1.12 (CVE-2011-2984)
- An arbitrary code execution vulnerability occurs because of an insecure DLL-loading issue in the 'ThinkPadSensor::Startup()' function. This could allow attackers to load a specially crafted DLL into the running process. This affects Firefox 3.6.20 and 3.1.12 (CVE-2011-2980)
- An information disclosure vulnerability occurs because of a cross-origin issue when 'RegExp.input' is set. This could cause data from other domains to be read. This affects Firefox 3.6.20 and 3.1.12 (CVE-2011-2983)

These vulnerabilities may be exploited if a user visits, or is redirected to a specially crafted web page. 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.

**RECOMMENDATIONS:**

The following actions should be taken:

- Upgrade vulnerable Mozilla products immediately after appropriate testing.
- 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/2011/mfsa2011-29.html>
- <http://www.mozilla.org/security/announce/2011/mfsa2011-30.html>
- <http://www.mozilla.org/security/announce/2011/mfsa2011-31.html>
- <http://www.mozilla.org/security/announce/2011/mfsa2011-32.html>
- <http://www.mozilla.org/security/announce/2011/mfsa2011-33.html>

**Security Focus:**

- <http://www.securityfocus.com/bid/49166>

**CVE:**

- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2378>
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2980>
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2982>
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2983>
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2984>
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2989>
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2990>
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2991>
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2992>
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2993>
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2985>
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2986>
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2987>
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2988>
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2984>
- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2981>