

*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:**

8/7/2013

**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 23.0
- Firefox Extended Support Release (ESR) versions prior to 17.0.8
- Thunderbird versions prior to 17.0.8
- Thunderbird Extended Support Release (ESR) versions prior to 17.0.8
- SeaMonkey versions prior to 2.20

**RISK:**

**Government:**

- Large and medium government entities: **High**
- Small government entities: **High**

**Businesses:**

- Large and medium government entities: **High**
- Small government 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:

- **Local Java applets may read contents of local file system (MFSA 2013-75)**  
An issue with Java applets where in some circumstances the applet could access files on the local system when loaded using the a [file:///](#) URI and violate file origin policy due to interaction with the codebase parameter.
- **Firefox full and stub installer DLL hijacking (MFSA 2013-74)**  
A specifically named DLL file on a Windows computer is placed in the default downloads directory with the Firefox installer, the Firefox installer will load this DLL file when it is launched.
- **Same-origin bypass with web workers and XMLHttpRequest (MFSA 2013-73)**  
A web worker can violate same-origin policy and bypass cross-origin checks through XMLHttpRequest. This could allow for cross-site scripting (XSS) attacks by web workers.
- **Wrong principal used for validating URI for some Javascript components (MFSA 2013-72)**  
Some Javascript components will perform checks against the wrong uniform resource identifier (URI) before performing security sensitive actions. This will return an incorrect location for the originator of the call. This could be used to bypass same-origin policy, allowing for cross-site scripting (XSS) or the installation of malicious add-ons from third-party pages.
- **Further Privilege escalation through Mozilla Updater (MFSA 2013-71)**  
The Mozilla Updater can be made to load a specific malicious DLL file from the local system. This DLL file can run in a privileged context through the Mozilla Maintenance Service's privileges, allowing for local privilege escalation. The DLL file can also run in an unprivileged context if the Mozilla Updater is run directly by a user in the same directory as the file. Local file system access is necessary in order for this issue to be exploitable.
- **Bypass of XrayWrappers using XBL Scopes (MFSA 2013-70)**  
XBL scopes can be used to circumvent XrayWrappers from within the Chrome on unprivileged objects. This allows web content to potentially confuse privileged code and weaken invariants and can lead to cross-site scripting (XSS) attacks.
- **CRMF requests allow for code execution and XSS attacks (MFSA 2013-69)**

There is a mechanism that can execute arbitrary code or a cross-site scripting (XSS) attack when Certificate Request Message Format (CRMF) request is generated in certain circumstances.

- **Document URI misrepresentation and masquerading (MFSa 2013-68)**

Through an interaction of frames and browser history it was possible to make the browser believe attacker-supplied content came from the location of a previous page in browser history. This allows for cross-site scripting (XSS) attacks by loading scripts from a misrepresented malicious site through relative locations and the potential access of stored credentials of a spoofed site.

- **Crash during WAV audio file decoding (MFSa 2013-67)**

The Address Sanitizer tool can cause a crash during the decoding of WAV format audio files in some instances. This crash is not exploitable but could be used for a denial of service (DOS) attack by malicious parties.

- **Buffer overflow in Mozilla Maintenance Service and Mozilla Updater (MFSa 2013-66)**

There are stack buffer overflows in both the Maintenance Service and the Mozilla Updater when unexpectedly long paths were encountered. A local attacker could pass these as command-line arguments to the Maintenance Service to crash either program and potentially lead to arbitrary code being run with the Administrator privileges used by the Maintenance Service and inherited by the Updater.

- **Buffer underflow when generating CRMF requests (MFSa 2013-65)**

There is a use-after-free problem when generating a Certificate Request Message Format (CRMF) request with certain parameters. This causes a potentially exploitable crash.

- **Use after free mutating DOM during SetBody (MFSa 2013-64)**

There is a use-after-free problem when the Document Object Model is modified during a SetBody mutation event. This causes a potentially exploitable crash.

- **Miscellaneous memory safety hazards (rv:23.0 / rv:17.0.8) (MFSa 2013-63)**

There are several memory safety bugs in the browser engine used in Firefox and other Mozilla-based products. Some of these bugs showed evidence of memory corruption under certain circumstances, and we presume that with enough effort at least some of these could be exploited to run arbitrary code.

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.

#### **RECOMMENDATIONS:**

The following actions should 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/>

<http://www.mozilla.org/security/announce/2013/mfsa2013-63.html>

<http://www.mozilla.org/security/announce/2013/mfsa2013-64.html>

<http://www.mozilla.org/security/announce/2013/mfsa2013-65.html>

<http://www.mozilla.org/security/announce/2013/mfsa2013-66.html>

<http://www.mozilla.org/security/announce/2013/mfsa2013-67.html>

<http://www.mozilla.org/security/announce/2013/mfsa2013-68.html>

<http://www.mozilla.org/security/announce/2013/mfsa2013-69.html>

<http://www.mozilla.org/security/announce/2013/mfsa2013-70.html>

<http://www.mozilla.org/security/announce/2013/mfsa2013-71.html>

<http://www.mozilla.org/security/announce/2013/mfsa2013-72.html>

<http://www.mozilla.org/security/announce/2013/mfsa2013-73.html>

<http://www.mozilla.org/security/announce/2013/mfsa2013-74.html>

<http://www.mozilla.org/security/announce/2013/mfsa2013-75.html>

##### **CVE:**

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1701>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1702>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1704>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1705>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1706>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1707>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1708>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1709>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1710>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1711>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1712>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1713>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1714>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1715>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1717>