

*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:**

1/9/2012

**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 18.0
- Firefox Extended Support Release (ESR) versions prior to 10.0.12 and 17.0.2
- Thunderbird versions prior to 17.0.2
- Thunderbird Extended Support Release (ESR) versions prior to 10.0.12 and 17.0.2
- SeaMonkey versions prior to 2.15

**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 (MFSA 2013-01) - several memory safety bugs in the browser engine used in Firefox and other Mozilla-based products have been identified. Some of these bugs showed evidence of memory corruption under certain circumstances, and some of these could be exploited to run arbitrary code.
- Use-after-free issue (MFSA 2013-02) - this issue affects the Address Sanitizer tool and could allow remote code execution.
- Buffer Overflow in Canvas (MFSA 2013-03) - there is an error when handling specific bad height and width values given through HTML. This issue causes a crash that may be exploitable.
- URL spoofing in address bar during page loads (MFSA 2013-04) - there is an issue where the displayed URL values within the address bar can be spoofed by a page during

loading. This could allow for phishing attacks where a malicious page can spoof the identity of another site.

- Use-after-free when displaying table with many columns and column groups (MFSA 2013-05) - this issue is caused by an array containing a large number of columns and column groups that causes the array to overwrite itself during rendering leading to a crash that may be exploitable.
- Touch events are shared across iframesAndroid (MFSA 2013-06) - this allows for information leakage and possibilities for cross-site scripting (XSS)
- Crash due to handling of SSL on threads (MFSA 2013-07) - there is a crashing issue found through Thunderbird when downloading messages over a Secure Sockets Layer (SSL) connection. The resulting crash is potentially exploitable.
- AutoWrapperChanger fails to keep objects alive during garbage collection (MFSA 2013-08) - the AutoWrapperChanger class fails to keep some javascript objects alive during garbage collection. This can lead to an exploitable crash allowing for arbitrary code execution.
- Compartment mismatch with quickstubs returned values (MFSA 2013-09) - there is a problem where jsval-returning quickstubs fail to wrap their return values, causing a compartment mismatch. This mismatch can cause garbage collection to occur incorrectly and lead to a potentially exploitable crash.
- Event manipulation in plugin handler to bypass same-origin policy (MFSA 2013-10) - the plugin handler can be manipulated by web content to bypass same-origin policy (SOP) restrictions. This can allow for clickjacking on malicious web pages.
- Address space layout leaked in XBL objects (MFSA 2013-11) - using the toString function of XBL objects can lead to inappropriate information leakage by revealing the address space layout instead of just the ID of the object. This layout information could potentially be used to bypass ASLR and other security protections.
- Buffer overflow in Javascript string concatenation (MFSA 2013-12) - an integer overflow is possible when calculating the length for a Javascript string concatenation, which is then used for memory allocation. This results in a buffer overflow, leading to a potentially exploitable memory corruption.
- Memory corruption in XBL with XML bindings containing SVG (MFSA 2013-13) - when using an XBL file containing multiple XML bindings with SVG content, a memory corruption can occur. In concern with remote XUL, this can lead to an exploitable crash.
- Chrome Object Wrapper (COW) bypass through changing prototype (MFSA 2013-14) - it is possible to change the prototype of an object and bypass Chrome Object Wrappers (COW) to gain access to chrome privileged functions. This could allow for arbitrary code execution.
- Privilege escalation through plugin objects (MFSA 2013-15) - it is possible to open a chrome privileged web page through plugin objects through interaction with SVG elements. This could allow for arbitrary code execution.
- Use-after-free in serializeToStream (MFSA 2013-16) - there is a use-after-free issue in XMLSerializer by the exposing of serializeToStream to web content. This can lead to arbitrary code execution when exploited.
- Use-after-free in ListenerManager (MFSA 2013-17) - there is a use-after-free issue within the ListenerManager when garbage collection is forced after data in listener objects has been allocated in some circumstances. This results in a use-after-free, which can lead to arbitrary code execution.
- Use-after-free in Vibrate (MFSA 2013-18) - there is a use-after-free issue when using the domDoc pointer within Vibrate library. This can lead to arbitrary code execution when exploited.
- Use-after-free in Javascript Proxy objects (MFSA 2013-19) - there is a garbage collection flaw in Javascript Proxy objects. This can lead to a use-after-free leading to arbitrary

code execution.

- Mis-issued TURKTRUST certificates (MFSa 2013-20) - TURKTRUST, a certificate authority in Mozilla's root program, had mis-issued two intermediate certificates to customers. The issue was not specific to Firefox but there was evidence that one of the certificates was used for man-in-the-middle (MITM) traffic management of domain names that the customer did not legitimately own or control. This issue was resolved by revoking the trust for these specific mis-issued certificates. 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/2013/mfsa2013-01.html>

<http://www.mozilla.org/security/announce/2013/mfsa2013-02.html>

<http://www.mozilla.org/security/announce/2013/mfsa2013-03.html>

<http://www.mozilla.org/security/announce/2013/mfsa2013-04.html>

<http://www.mozilla.org/security/announce/2013/mfsa2013-05.html>

<http://www.mozilla.org/security/announce/2013/mfsa2013-06.html>

<http://www.mozilla.org/security/announce/2013/mfsa2013-07.html>

<http://www.mozilla.org/security/announce/2013/mfsa2013-08.html>

<http://www.mozilla.org/security/announce/2013/mfsa2013-09.html>

<http://www.mozilla.org/security/announce/2013/mfsa2013-10.html>

<http://www.mozilla.org/security/announce/2013/mfsa2013-11.html>

<http://www.mozilla.org/security/announce/2013/mfsa2013-12.html>

<http://www.mozilla.org/security/announce/2013/mfsa2013-13.html>

<http://www.mozilla.org/security/announce/2013/mfsa2013-14.html>

<http://www.mozilla.org/security/announce/2013/mfsa2013-15.html>

<http://www.mozilla.org/security/announce/2013/mfsa2013-16.html>

<http://www.mozilla.org/security/announce/2013/mfsa2013-17.html>

<http://www.mozilla.org/security/announce/2013/mfsa2013-18.html>

<http://www.mozilla.org/security/announce/2013/mfsa2013-19.html>

<http://www.mozilla.org/security/announce/2013/mfsa2013-20.html>

### **CVE:**

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0743>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0744>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0745>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0746>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0747>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0748>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0749>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0750>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0751>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0752>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0753>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0754>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0755>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0756>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0757>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0758>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0760>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0761>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0762>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0763>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0764>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0767>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0768>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0769>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0770>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0771>

**SecurityFocus:**

<http://www.securityfocus.com/bid/57185>