

*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:**

03/08/2013

**SUBJECT:**

Vulnerability in Mozilla Products Could Allow Remote Code Execution

**OVERVIEW:**

A vulnerability has 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 19.0.2

Firefox Extended Support Release (ESR) versions prior to 17.0.4

Thunderbird versions prior to 17.0.4

Thunderbird Extended Support Release (ESR) versions prior to 17.0.4

SeaMonkey versions prior to 2.16.1

**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:**

A use-after-free vulnerability has been discovered in Mozilla Firefox, Thunderbird, and SeaMonkey. This vulnerability exists within the HTML editor when a content script is run by the document.execCommand() function while internal editor operations are occurring.

Successful exploitation of this vulnerability 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:**

**Security Focus:**

<http://www.securityfocus.com/bid/58391>

**Mozilla:**

<http://www.mozilla.org/security/announce/2013/mfsa2013-29.html>

**CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0787>