

*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.*

**TLP: WHITE**

**Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.**

<http://www.us-cert.gov/tlp/>

**DATE(S) ISSUED:**

03-23-2015

**SUBJECT:**

Multiple Vulnerabilities in Mozilla Firefox and SeaMonkey Could Allow for Remote Code Execution

**OVERVIEW:**

Multiple vulnerabilities have been identified in Mozilla Firefox and SeaMonkey which could allow for remote code execution. Mozilla Firefox is a web browser used to access the Internet and SeaMonkey is an all-in-one set of programs used for accessing the internet. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. 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.

**THREAT INTELLIGENCE**

There are currently no reports of these vulnerabilities being exploited in the wild.

**SYSTEM AFFECTED:**

- Mozilla Firefox versions prior to 36.0.3
- Firefox versions prior ESR 31.5.2
- SeaMonkey versions prior 2.33.1

**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**

**TECHNICAL SUMMARY:**

Two Vulnerabilities have been reported in Mozilla Firefox and SeaMonkey. Details of the vulnerabilities are as follows:

- A remote-code execution vulnerability with the use of an out-of-bounds read/write error. This vulnerability occurs due to an error in the implementation of the Javascript just-in-time compilation's typed array bounds checking. Once exploited, an attacker can run arbitrary code remotely as the logged on user or cause denial-of-service conditions. (CVE-2015-0817)

- A privilege-escalation vulnerability using SVG format content navigation processing. This processing can be used by the attacker to bypass the same-origin policy and then remotely execute arbitrary code on the system. (CVE-2015-0818)

**RECOMMENDATIONS:**

The following actions should be taken:

- Upgrade to latest versions of Mozilla Firefox and SeaMonkey.
- Run all software as a non-privileged user to diminish effects of a successful attack

**REFERENCES:****Mozilla:**

<https://www.mozilla.org/en-US/security/advisories/mfsa2015-29/>

<https://www.mozilla.org/en-US/security/advisories/mfsa2015-28/>

**CVE:**

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0817>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0818>

**SecurityFocus:**

<http://www.securityfocus.com/bid/73236>

<http://www.securityfocus.com/bid/73625>

**TLP: WHITE**

**Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.**

<http://www.us-cert.gov/tlp/>