

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:

05/13/2015

SUBJECT:

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

OVERVIEW:

Multiple vulnerabilities have been identified in Mozilla Firefox, Firefox ESR, and Thunderbird, which could allow for remote code execution. Mozilla Firefox is a web browser used to access the Internet, Firefox ESR is a version of the web browser intended to be deployed in large organizations, and Mozilla Thunderbird is an email client. 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.

SYSTEMS AFFECTED:

- Mozilla Firefox versions prior to 38
- Firefox ESR versions prior to 31.7
- Thunderbird versions prior to 31.7

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:

Multiple vulnerabilities have been discovered in Mozilla Firefox, Firefox ESR, and Thunderbird that an attacker could exploit to execute arbitrary code in the context of the vulnerable application, crash affected applications, disclose sensitive information, bypass the same-origin policy and other security restrictions, and perform unauthorized actions. These vulnerabilities can be exploited if a user visits or is redirected to a specially crafted webpage or opens a specially crafted file. Details of these vulnerabilities are as follows:

- A heap-based buffer-overflow vulnerability exists in the 'SVGTextFrame'. Specifically, this issue occurs during the rendering of SVG format graphics when combined with specific CSS properties on a page. [CVE-2015-2710]
- A security-bypass vulnerability exists because it ignores Referrer policy when links opened by middle-click of mouse and context menu under certain circumstances. [CVE-2015-2711]
- An Out-of-bounds read and write vulnerability exists because it fails to properly validate the 'asm.js' file. [CVE-2015-2712]
- A heap-based buffer-overflow vulnerability exists in the 'SetBreaks'. Specifically, this issue occurs due to a use-after-free error during the processing of text when vertical text is enabled. [CVE-2015-2713]
- An information-disclosure vulnerability exists because it fails to check whether sensitive URL encoded information is being written to Android logcat that is encoded as part of logged URL strings. [CVE-2015-2714]
- A heap-based buffer-overflow vulnerability exists in the 'nsThreadManager::RegisterCurrentThread'. Specifically, this issue occurs due to a use-after-free error during the shutdown process. [CVE-2015-2715]
- A buffer-overflow vulnerability occurs when parsing compressed XML content. [CVE-2015-2716]
- An integer buffer-overflow vulnerability occurs when parsing invalid metadata in MP4 video files. Specifically, this issue occurs due to an out-of-bounds read error in the 'libstagefright' library. This may lead to heap-based buffer-overflow. [CVE-2015-2717]
- A same-origin security-bypass vulnerability exists due to the way WebChannel.jsm handles message traffic. [CVE-2015-2718]
- A security vulnerability occurs during the fixing of CVE-2015-0833. [CVE-2015-2720]

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate updates provided by Mozilla Firefox and Thunderbird to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCES:

Mozilla:

<https://www.mozilla.org/en-US/security/advisories/mfsa2015-46>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-48>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-49>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-50>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-51>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-52>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-53>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-54>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-55>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-56>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-57>

<https://www.mozilla.org/en-US/security/advisories/mfsa2015-58>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2708>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2709>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2710>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2711>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2712>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2713>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2714>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2715>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2716>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2717>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2718>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2720>

Security Focus:

<http://www.securityfocus.com/bid/74611>

<http://www.securityfocus.com/bid/74615>

TLP: WHITE

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

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