

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 ISSUED:

07/03/2015

SUBJECT:

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

OVERVIEW:

Multiple vulnerabilities have been identified in Mozilla Firefox 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. 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 39
- Firefox ESR versions prior to 31.8
- Thunderbird versions prior to 38.1

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:

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:

- Multiple unspecified memory-corruption vulnerabilities that exist in the browser engine. [CVE-2015-2724, CVE-2015-2725, CVE-2015-2726]
- A local security-bypass vulnerability because opening hyperlinks on a page with the mouse and specific keyboard key combinations could allow a Chrome privileged URL to be opened without context restrictions being preserved. [CVE 2015-2727]
- A security-bypass vulnerability occurs due to an error in Network Security Services (NSS) where the client allows for a ECDHE_ECDSA exchange where the server does not send its ServerKeyExchange message instead of aborting the handshake. [CVE-2015-2721]
- A privilege escalation vulnerability occurs due to broken behavior in Mozilla's PDF file viewer. [CVE-2015-2743]
- An information-disclosure vulnerability occurs while reviewing Firefox crash reports. This issue exists because the OS X crash reports contain the native key and key press information that was being entered when the crash occurred. [CVE-2015-2742]
- A security-bypass vulnerability occurs when an overridable error is encountered. An attacker can exploit this issue to override a pinned certificate. [CVE-2015 2741]
- Multiple unspecified memory-corruption vulnerabilities affect the applications. Specifically, these issues affect the 'CairoTextureClientD3D9::BorrowDrawTarget', 'nsZipArchive::BuildFileList', 'rx::d3d11::SetBufferData', 'YCbCrImageDataDeserializer::ToDataSourceSurface', 'ArrayBufferBuilder::append', 'nsXMLHttpRequest::AppendToResponseText' functions and 'nsZipArchive.cpp' source file. [CVE-2015-2734, CVE-2015-2735, CVE-2015-2736, CVE-2015-2737, CVE-2015-2738, CVE-2015-2739, CVE-2015-2740]
- Multiple use-after-free vulnerabilities occur when using XMLHttpRequest in concert with either shared or dedicated workers. [CVE-2015-2722, CVE-2015-2723]
- A security-bypass vulnerability occurs because Elliptical Curve Cryptography (ECC) multiplication for Elliptic Curve Digital Signature Algorithm (ECDSA) signature in Network Security Services (NSS) fails to handle certain signatures correctly. [CVE-2015-2730]
- A use-after-free vulnerability occurs in Content Policy due to microtask execution error. [CVE-2015-2731]
- An out-of-bound read vulnerability occurs while computing an oscillator rendering range in Web Audio. [CVE-2015-2729]
- A memory corruption vulnerability occurs due to a type confusion in Indexed Database Manager. Specifically, this issue affects the 'mozilla::dom::indexedDB::IndexedDatabaseManager()' function. [CVE-2015-2728]

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/mfsa2015-59/>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-60/>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-61/>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-62/>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-63/>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-64/>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-65/>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-66/>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-67/>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-68/>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-69/>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-71/>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2721>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2722>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2723>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2724>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2725>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2726>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2727>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2728>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2729>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2730>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2731>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2734>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2735>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2736>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2737>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2738>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2739>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2740>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2741>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2742>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2743>

TLP: WHITE

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

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