

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/tp/>

DATE(S) ISSUED:

4/1/2015

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 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.

SYSTEM AFFECTED:

- Mozilla Firefox versions prior to 37
- Firefox ESR versions prior 31.6
- Thunderbird versions prior 31.6

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:

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

Mozilla Firefox for Android is prone to a DNS poisoning attack as it uses an insufficiently random algorithm when generating random numbers for the unique identifier (CVE-2015-0800, CVE-2012-2808).

Mozilla Firefox, Firefox ESR, and Thunderbird are prone to a same-origin bypass as a flaw in the anchor navigation of a page could allow bypassing of same-origin policy protections (CVE-2015-0801).

Mozilla Firefox is prone to an escalation of privilege and arbitrary code execution if coupled with another vulnerability allowing for web content to reference these privileged windows (CVE-2015-0802).

Mozilla Firefox is prone to remote-code execution due to a use after free type confusion flaw after binding or setting attributes of a *source* element (CVE-2015-0803, CVE-2015-0804).

Mozilla Firefox is prone to memory corruption crashes during 2D graphics rendering due to problems in Off Main Thread Compositing (CVE-2015-0805, CVE-2015-0806).

Mozilla Firefox, Firefox ESR, and Thunderbird are prone to a potential Cross-site request forgery (XSRF) attack from malicious websites affecting the *sendBeacon()* requests (CVE-2015-0807).

Mozilla Firefox is prone to incorrect memory management for simple-type arrays in WebRTC (CVE-2015-0808).

Mozilla Firefox on OS X is prone to a potential clickjacking by making the cursor invisible through flash content and then replaced it through the layering of HTML content (CVE-2015-0810).

Mozilla Firefox is prone to an information disclosure due to an out of bounds read in the QCMS color management library while transforming images with certain parameters (CVE-2015-0811).

Mozilla Firefox is prone to an a man-in-the-middle (MITM) attack from a spoofed Mozilla sub-domain which could bypass user approval messages installing a Firefox lightweight theme (CVE-2015-0812).

Mozilla Firefox on Linux is prone to a use-after-free when playing certain MP3 format audio files on the web using the Fluendo MP3 plugin for GStreamer (CVE-2015-0813).

Mozilla Firefox, Firefox ESR, and Thunderbird are prone to potential memory corruption and arbitrary code execution due to several memory safety bugs (CVE-2015-0814, CVE-2015-0815).

Mozilla Firefox, Firefox ESR, and Thunderbird are prone to a privilege escalation and potential arbitrary code execution from improper handling of *resource://* documents (CVE-2015-0816).

RECOMMENDATIONS:

The following actions should be taken:

Upgrade to latest versions of Mozilla Firefox and Thunderbird after appropriate testing.

Run all software as a non-privileged user to diminish effects of a successful attack.

Remind users not to click links from unknown sources, or to click links without verifying the intended destination.

REFERENCES:

Mozilla:

<https://www.mozilla.org/en-US/security/advisories/mfsa2015-30>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-31>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-32>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-33>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-34>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-35>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-36>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-37>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-38>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-39>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-40>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-41>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-42>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0800>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0801>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0802>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0803>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0804>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0805>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0806>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0807>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0808>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0810>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0811>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0812>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0813>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0814>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0815>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0816>

TLP: WHITE

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

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