

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:

02/25/2015

SUBJECT:

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

EXECUTIVE SUMMARY:

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, 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.

THREAT INTELLIGENCE:

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

SYSTEM AFFECTED:

Mozilla Firefox versions prior to 36

Firefox versions prior ESR 31.5

Thunderbird versions prior 31.5

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:

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

Mozilla Firefox is prone to a denial-of-service vulnerability. (CVE-2015-0830, CVE-2015-0824, CVE-2015-0826, CVE-2015-0831, CVE-2015-0823).

Mozilla Firefox is prone to a disclosure of credentials through a Man-in-the-middle (MITM) attack (CVE-2015-0834).

Mozilla Firefox is prone to a security bypass vulnerability (CVE-2015-0832, CVE-2015-0820).

Mozilla Firefox and Thunderbird are prone to a security vulnerability because 'UITour: onPageEvent' fails to ignore API calls from background tabs. (CVE-2015-0819).

Mozilla Firefox and Thunderbird are prone to an arbitrary file read vulnerability allowing a user to upload a readable file to a malicious site. (CVE-2015-0822).

Mozilla Firefox and Thunderbird are prone to an unspecified memory-corruption vulnerability which may allow an attacker to execute arbitrary code. (CVE-2015-0836, CVE-2015-0835).

Mozilla Firefox, Thunderbird, and Firefox ESR are prone to a vulnerability which may allow an attacker to execute arbitrary code. (CVE-2015-0833, CVE-2015-0828, CVE-2015-0829, CVE-2015-0825, CVE-2015-0827).

Mozilla Firefox is prone to Local files or privileged URLs in pages being opened in new tabs. (CVE-2015-0821).

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Mozilla 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 click links from unknown sources, or to click links without verifying the intended destination.

REFERENCES:

Mozilla:

<https://www.mozilla.org/en-US/security/advisories/mfsa2015-11/>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-12/>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-13/>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-14/>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-15/>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-16/>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-17/>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-18/>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-19/>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-20/>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-21/>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-22/>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-23/>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-24/>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-25/>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-26/>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-27/>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0819>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0820>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0821>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0822>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0823>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0824>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0825>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0826>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0827>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0828>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0829>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0830>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0831>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0832>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0833>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0834>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0835>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0836>

SecurityFocus:

<http://www.securityfocus.com/bid/72741>
<http://www.securityfocus.com/bid/72742>
<http://www.securityfocus.com/bid/72742>
<http://www.securityfocus.com/bid/72743>
<http://www.securityfocus.com/bid/72746>
<http://www.securityfocus.com/bid/72747>
<http://www.securityfocus.com/bid/72748>
<http://www.securityfocus.com/bid/72749>
<http://www.securityfocus.com/bid/72750>
<http://www.securityfocus.com/bid/72752>
<http://www.securityfocus.com/bid/72753>
<http://www.securityfocus.com/bid/72754>
<http://www.securityfocus.com/bid/72756>
<http://www.securityfocus.com/bid/72757>
<http://www.securityfocus.com/bid/72758>
<http://www.securityfocus.com/bid/72759>

TLP: WHITE

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

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