

*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:**

09/22/2015

**SUBJECT:**

Multiple Vulnerabilities in Mozilla Firefox Could Allow for Arbitrary Code Execution

**OVERVIEW:**

Multiple vulnerabilities have been identified in Mozilla Firefox, which could allow for arbitrary 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. Firefox OS is the mobile operating system developed by Mozilla. 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 41
- Firefox ESR versions prior to 38.3
- Firefox OS versions prior to 2.5

**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:**

Mozilla has confirmed multiple vulnerabilities in Firefox, Firefox ESR, and Firefox OS. Exploitation of these vulnerabilities could allow for arbitrary code execution in the context of the logged on user or vulnerable application, crash the affected application, disclose sensitive information, bypass the same-origin policy and other security restrictions, and perform unauthorized actions. These vulnerabilities could 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:

- Two unspecified memory corruption vulnerabilities exist that could lead to arbitrary code execution (CVE-2015-4500, CVE-2015-4501)
- One vulnerability that could lead to exposure of memory or private data to malicious servers (CVE-2015-4503)
- One out of bounds read vulnerability in QCMS color management library which could lead to information disclosure (CVE-2015-4504)
- One vulnerability which could potentially lead to site attribute spoofing by pasting a URL with an unknown scheme ( CVE-2015-4476)
- One vulnerability which could lead to arbitrary file manipulation by local user through the Mozilla updater (CVE-2015-4505)
- One vulnerability in libvpx while parsing vp9 format video which could lead to buffer overflow (CVE-2015-4506)
- One vulnerability when using the debugger with SavedStacks in Javascript could lead to potentially exploitable crash (CVE-2015-4507)
- One vulnerability in reader mode which could lead to spoof the URL displayed in the addressed bar (CVE-2015-4508)
- One use-after-free vulnerability exists when using a shared worker with indexedDB which could lead to a potentially exploitable crash (CVE-2015-4510)
- One buffer overflow vulnerability exists while decoding WebM videos which could lead to a potentially exploitable crash
- One use-after-free vulnerability exists while manipulating HTML media content which could lead to a potentially exploitable crash (CVE-2015-4509)
- One out of bounds read vulnerability exists while utilizing 2D canvas display on Linux 16-bit color depth systems (CVE-2015-4512)
- One vulnerability exists in the way data is passed to a scripted proxy which violates the specifications set in place (CVE-2015-4502)
- One vulnerability exists in Gecko's implementation of ECMAScript 5 API which could lead to arbitrary code execution (CVE-2015-4516)
- One vulnerability exists in the way dragged and dropped images are handled which could lead to information leakage (CVE-2015-4519)
- One vulnerability exists in the way Cross-origin resource sharing(CORS) preflight request headers are handled which could lead to CORS security checks being bypassed (CVE-2015-4520)
- Multiple vulnerabilities were discovered through the use of code inspector which could lead to memory safety issues or bypassing of overflow checks (CVE-2015-4517, CVE-2015-4521, CVE-2015-4522, CVE-2015-7174, CVE-2015-7175, CVE-2015-7176, CVE-2015-7177, CVE-2015-7180)
- Two vulnerabilities in the libGLES portion of the ANGEL graphics library which could lead to potentially exploitable crashes (CVE-2015-7178, CVE-2015-7179)
- One vulnerability in the High Resolution Time API that could lead to information disclosure.

## **RECOMMENDATIONS:**

The following actions should be taken:

- Apply appropriate updates 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 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/mfsa2015-96>  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-97>  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-98>  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-99>  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-100>  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-101>  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-102>  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-103>  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-104>  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-105>  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-106>  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-107>  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-108>  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-109>  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-110>  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-111>  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-112>  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-113>  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-114>

### CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4500>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4501>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4504>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4503>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4476>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4505>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4506>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4507>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4508>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4510>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4509>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4512>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4502>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4516>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4519>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4517>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4521>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4522>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7174>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7175>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7176>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7177>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7178>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7179>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4520>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7180>

**TLP: WHITE**

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

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