

*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:**

12/15/2015

**SUBJECT:**

Multiple Vulnerabilities in Mozilla Firefox Could Allow for Arbitrary Code Execution

**OVERVIEW:**

Multiple vulnerabilities have been identified in Mozilla Firefox and Firefox ESR which could allow for arbitrary code execution. Mozilla Firefox is a web browser used to access the Internet. Mozilla Firefox ESR is a version of the web browser intended to be deployed in large organizations. Exploit of these issues can allow an attacker to bypass security restrictions and perform unauthorized actions, obtain sensitive information, bypass same-origin policy restrictions to access data, and execute arbitrary code in the context of the affected application. Failed exploit attempts will likely result in denial-of-service conditions.

**THREAT INTELLIGENCE:**

There are currently no reports of this vulnerability being exploited in the wild.

**SYSTEMS AFFECTED:**

- Mozilla Firefox versions prior to 43
- Mozilla Firefox ESR versions prior to 38.5

**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 and Firefox ESR. 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:

- Security-bypass vulnerability exists. Specifically, the issue occurs due to a cross-origin restriction bypass when using 'data: and view-source:' uri scheme. An attacker can exploit this issue to read data from cross-site URLs and local files. [CVE-2015-7214]
- Multiple buffer-overflow vulnerabilities exist because it fails to adequately bounds-check user-supplied data before copying it into an insufficiently sized buffer. Specifically, these

issues affect the 'libstagefright' library. An attacker can exploit these issues by sending cover metadata. [CVE-2015-7222]

- Integer-overflow vulnerability exists because it fails to adequately bounds-check user-supplied data before copying it into an insufficiently sized buffer. Specifically, this issue affects the 'MPEG4Extractor::readMetaData'. [CVE-2015-7213]
- Information-disclosure vulnerability exists. Specifically, this issue occurs due to an underflow in the 'RTPReceiverVideo::ParseRtpPacket'. [CVE-2015-7205]
- Integer-overflow vulnerability exists because it fails to adequately bounds-check user-supplied data before copying it into an insufficiently sized buffer. Specifically, this issue occurs due to a 'memset' crash in the 'mozilla::layers::BufferTextureClient::AllocateForSurface'. [CVE-2015-7212]
- Multiple memory-corruption vulnerabilities occur due to memory-safety errors. Specifically, these issues affect the browser engine. [CVE-2015-7201, CVE-2015-7202]
- A security vulnerability because it uses vulnerable Jasper. [CVE-2015-7216]
- Security bypass vulnerability because it uses vulnerable TGA decoders of 'gdk-pixbuf' gnome library. An attacker can exploit this issue to cause heap-based buffer overflow and denial-of-service vulnerabilities. [CVE-2015-7217]
- A denial-of-service vulnerability occurs because of an error in JavaScript variable assignments. Specifically, this issue occurs due to an implementation error with unboxed objects and property storing in the JavaScript engine. An attacker can exploit this issue to crash the affected application. [CVE-2015-7204] *Note: This issue affects only Firefox 41 and later.*
- A same-origin security-bypass vulnerability occurs when 'performance.getEntries()' is used along with an iframe to host a page. An attacker can exploit this issue by navigating back in history through script when loading cache to read cross-origin URLs. [CVE-2015-7207]
- A security-bypass vulnerability occurs when ASCII code 11 for vertical tab is stored in a cookie. An attacker can exploit this issue to set cookie values and read cookie data. [CVE-2015-7208]
- A cross-origin information disclosure vulnerability occurs due to the error events in web workers. An attacker can exploit this issue to gain authentication tokens. [CVE-2015-7215]
- A security-bypass vulnerability occurs because it fails to properly parse Hash (#) symbol in data URI. An attacker can exploit this issue to perform spoofing attacks. [CVE-2015-7211]
- A denial-of-service vulnerability occurs due to an integer underflow error. Specifically, this issue occurs when a malicious HTTP/2 header frame is received with a single byte. [CVE-2015-7218]
- A denial-of-service vulnerability occurs due to an integer underflow error. Specifically, this issue occurs when a malicious HTTP/2 PushPromise frame is received with miscalculated length of decompressed buffer. [CVE-2015-7219]
- A buffer-overflow vulnerability exists because it fails to adequately bounds-check user-supplied data before copying it into an insufficiently sized buffer. Specifically, this issue affects the 'OOM' in 'DirectWriteFontInfo::LoadFontFamilyData'. [CVE-2015-7203]
- A buffer-overflow vulnerability exists because it fails to adequately bounds-check user-supplied data before copying it into an insufficiently sized buffer. Specifically, this issue affects the 'XDRBuffer::grow'. [CVE-2015-7220]
- A buffer-overflow vulnerability exists because it fails to adequately bounds-check user-supplied data before copying it into an insufficiently sized buffer. Specifically, this issue affects the 'nsDeque::GrowCapacity'. [CVE-2015-7221]
- A privilege escalation vulnerability exists due to an error in mechanism in WebExtension APIs. An attacker can exploit this issue to execute arbitrary code with elevated privileges, information disclosure and cause cross-site scripting attacks. [CVE-2015-7223]

## 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/mfsa2015-134/>  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-135/>  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-136/>  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-137/>  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-139/>  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-140/>  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-141/>  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-142/>  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-144/>  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-148/>  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-145/>  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-146/>  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-147/>  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-149/>  
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-143/>

### CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7214>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7222>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7213>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7205>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7212>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7201>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7202>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7216>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7214>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7204>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7207>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7208>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7215>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7211>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7219>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7203>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7220>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7221>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7223>

### TLP: WHITE

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

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

