

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:

08/11/2015

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 40
- Firefox ESR versions prior to 38.2
- Firefox OS 2.2

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, which an attacker could exploit to execute arbitrary code 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:

- Multiple unspecified memory-corruption vulnerabilities exist in the browser engine, which could allow for the arbitrary code execution. (CVE-2015-4473, CVE-2015-4474)
- Multiple buffer overflow vulnerabilities exist in the Libvpx library, which could allow for arbitrary code execution. (CVE-2015-4485, CVE-2015-4486, CVE-2015-4491)
- A use-after-free memory corruption vulnerability occurs when handling audio through the Web Audio API, which could allow for arbitrary code execution. (CVE-2015-4477)

- A use-after-free vulnerability occurs when recursively calling the 'open()' function on an 'XMLHttpRequest' request in a SharedWorker. (CVE-2015-4492)
- Multiple memory corruption vulnerabilities exist in 'nsTSubstring::ReplacePrep', 'StyleAnimationValue::operator=', and 'nsTArray_Impl' (CVE-2015-4487, CVE-2015-4488, CVE-2015-4489)
- A cross-site scripting vulnerability exists in the Content Security Policy, which could allow for arbitrary code execution. (CVE-2015-4490)
- Multiple integer-overflow vulnerabilities exist in 'libstagefright', which could allow for arbitrary code execution. (CVE-2015-4479, CVE-2015-4480, CVE-2015-4493)
- Arbitrary file-overwrite vulnerability occurs due to a race condition involving the Mozilla Maintenance Service, which could allow an attacker to write arbitrary files. (CVE-2015-4481)
- Same-origin policy by-pass while parsing JSON, which could allow for properties to be modified with arbitrary values. (CVE-2015-4478)
- Multiple out-of-bounds memory corruption vulnerabilities exist, which could allow an attacker to obtain sensitive information or cause a denial of service. (CVE-2015-4475, CVE-2015-4482)
- Shared Memory Access vulnerability exists regarding the 'void js::jit::AssemblerX86Shared::lock_addl' function, which could result in a denial of service. (CVE-2015-4484)
- Man-in-the-middle vulnerability exists when using a POST with the 'feed:' protocol, which could allow for information disclosure. (CVE-2015-4483)

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate updates provided by Mozilla Firefox 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/mfsa2015-69/>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-70/>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-71/>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-72/>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-73/>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-74/>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-75/>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-76/>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-77/>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-78/>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-79/>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4473>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4474>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4475>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4477>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4478>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4479>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4480>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4481>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4482>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4483>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4484>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4485>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4486>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4487>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4488>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4489>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4490>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4491>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4492>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4493>

TLP: WHITE

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

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