

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:

01/27/2016

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. Exploitation 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 these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- Mozilla Firefox versions prior to 44
- Mozilla Firefox ESR versions prior to 38.6

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Medium

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:

- Multiple memory-corruption vulnerabilities that occur due under certain circumstances. Specifically, these issues affect the browser engine. (CVE-2016-1930, CVE-2016-1931)

- A denial-of-service vulnerability occurs because of an error in the image parsing code during the de-interlacing of a maliciously crafted GIF formatted image resulting in a possible integer overflow. (CVE-2016-1933)
- A buffer-overflow vulnerability, that could result in a potentially exploitable crash exists when rendering WebGL content. (CVE-2016-1935)
- A security-bypass vulnerability exists, that allows for control characters to be set in cookie names. This vulnerability could result in a web server to incorrectly handle the altered cookie. (CVE-2015-7208, CVE-2016-1939)
- Security-bypass vulnerability exists when an address bar spoofing condition occurs for stored data: URL shortcuts/bookmarks, as a result of an error in how Firefox on Android devices handle data: URLs. The spoofing issue occurs when a data: URL is opened from a stored shortcut/bookmark, and the address bar continues to show the data: URL even if the content redirects to another page. (CVE-2016-1940)
- A security vulnerability exists due to a lack of delay following user click events in the protocol handler dialog, resulting in double click events to be treated as two single click events. This issue could result in unintentional user interactions. (CVE-2016-1937)
- A security vulnerability exists because calculations with mp_div and mp_exptmod in Network Security Services (NSS) can produce wrong results in some circumstances. These functions are used within NSS for a variety of cryptographic division functions, leading to potential cryptographic weaknesses. (CVE-2016-1938)
- A security vulnerability exists impacting Firefox for OSX where a delay following click events between the download dialog getting focus and the button getting enabled was too short. This issue could possibly allow for unintentional user actions such as the running of downloaded software. (CVE-2016-1941) Note: This issue only affects OS X installations. Windows, Linux, and Android installations are unaffected by it.
- Multiple security-bypass vulnerability exists for address bar spoofing attacks, that can lead to potential spoofing by malicious domains. (CVE-2016-1943, CVE-2016-1942)
- Multiple memory-manipulation vulnerabilities were discovered through code inspection, that could allow for arbitrary code execution. The issues include the following: a memory safety issue in the ANGLE graphics library, a wild pointer flaw when handling zip files, and an integer overflow during metadata parsing in Mozilla's use of the libstagefright library. (CVE-2016-1944, CVE-2016-1945, CVE-2016-1946)
- A security vulnerability exists due to an Application Reputation service being disabled in Firefox version 43. The disabling of the service removed the ability of Safe Browsing to warn against potentially malicious downloads. (CVE-2016-1947) Note: Only Firefox version 43 is impacted.
- A security vulnerability exists due to Lightweight themes on Firefox for Android not verifying a secure connection, allowing for the themes to be installed over an unencrypted connection and possibly allowing for a man-in-the-middle (MITM) attacks. (CVE-2016-1948)

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/mfsa2016-01>
<https://www.mozilla.org/en-US/security/advisories/mfsa2016-02>
<https://www.mozilla.org/en-US/security/advisories/mfsa2016-03>
<https://www.mozilla.org/en-US/security/advisories/mfsa2016-04>
<https://www.mozilla.org/en-US/security/advisories/mfsa2016-05>
<https://www.mozilla.org/en-US/security/advisories/mfsa2016-06>
<https://www.mozilla.org/en-US/security/advisories/mfsa2016-07>
<https://www.mozilla.org/en-US/security/advisories/mfsa2016-08>
<https://www.mozilla.org/en-US/security/advisories/mfsa2016-09>
<https://www.mozilla.org/en-US/security/advisories/mfsa2016-10>
<https://www.mozilla.org/en-US/security/advisories/mfsa2016-11>
<https://www.mozilla.org/en-US/security/advisories/mfsa2016-12>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7208>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1930>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1931>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1933>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1935>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1937>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1938>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1939>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1940>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1941>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1942>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1943>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1944>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1945>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1946>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1947>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1948>

Security Focus:

<http://www.securityfocus.com/bid/81947>
<http://www.securityfocus.com/bid/81948>
<http://www.securityfocus.com/bid/81949>
<http://www.securityfocus.com/bid/81950>
<http://www.securityfocus.com/bid/81951>
<http://www.securityfocus.com/bid/81952>
<http://www.securityfocus.com/bid/81953>
<http://www.securityfocus.com/bid/81954>
<http://www.securityfocus.com/bid/81955>
<http://www.securityfocus.com/bid/81956>

<http://www.securityfocus.com/bid/81957>
<http://www.securityfocus.com/bid/81958>

TLP: WHITE

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

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