

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:

11/16/2016

SUBJECT:

Multiple Vulnerabilities in Mozilla Firefox Could Allow for Arbitrary Code Execution

OVERVIEW:

Multiple vulnerabilities have been identified in Mozilla Firefox and Firefox Extended Support Release (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 the most severe of these vulnerabilities could allow an attacker to bypass same-origin policy restrictions to access data, and execute arbitrary code in the context of the affected application.

THREAT INTELLIGENCE:

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

SYSTEM AFFECTED:

- Mozilla Firefox versions prior to 50
- Mozilla Firefox ESR versions prior to 45.3

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: Low

TECHNICAL SUMMARY:

Mozilla has confirmed multiple vulnerabilities in Firefox and Firefox Extended Support Release (ESR). Exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution, 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:

Mozilla Firefox Vulnerabilities

- A denial-of-service vulnerability. Specifically, this issue occurs during URL parsing. (CVE-2016-5292)
- Multiple denial-of-service vulnerabilities due to an use-after-free errors during DOM operations. Specifically, these issues occurs in 'nsINode::ReplaceOrInsertBefore'. (CVE-2016-9067) (CVE-2016-9069)
- A denial-of-service vulnerability due to an use-after free error during web animations. Specifically, this issue occurs in 'nsRefreshDriver'. (CVE-2016-9068)
- A security-bypass vulnerability exists only for 64-bit Windows operating system. Specifically, this issue occurs when a new Firefox profile is created on 64-bit Windows installations, the sandbox for 64-bit NPAPI plugins is not enabled by default. (CVE-2016-9072)
- A privilege-escalation vulnerability. Specifically, this issue affects the mozAddonManager API. (CVE-2016-9075)
- A security-bypass vulnerability. Specifically, this issue affects 'feDisplacementMap' filter. Successful exploits may allow an attackers to perform timing attacks. (CVE-2016-9077)
- A privilege-escalation vulnerability which only affects Windows operating systems exists, which if successful exploited may allow an attackers to read arbitrary files as SYSTEM. (CVE-2016-5295)
- A denial-of-service vulnerability that only affects Firefox for Android exists. Specifically, this issue affects the SSL indicator. Successful exploits may allow an attacker to mislead the user about the real URL visited. (CVE-2016-5298)
- A security vulnerability that only affects Firefox for Android exists in the Firefox AuthTokens. Specifically, this issue occurs due to an insecure permission. (CVE-2016-5299)
- A security vulnerability that only affects Firefox for Android exists in the API key(glocation). Specifically, this issue occurs due to an insecure permission. (CVE-2016-9061)
- An information-disclosure vulnerability that only impacts Firefox for Android exists. Specifically, this issue affects the browser.db and browser.db-wal files. (CVE-2016-9062)
- A security-bypass vulnerability. An attacker can exploit this issue by loading specially crafted page to the sidebar through a bookmark. (CVE-2016-9070)
- A security-bypass vulnerability because it fails to specify 'format': 'relativeUrl'. Specifically, this issue affects the 'windows.create' schema. (CVE-2016-9073)
- A security-bypass vulnerability due to an address bar spoofing. An attacker can exploit this issue using <select> dropdown menu. (CVE-2016-9076)
- An integer-overflow vulnerability. Specifically, this issue occurs during the parsing of XML using the Expat library. (CVE-2016-9063)
- A security vulnerability due to an Content Security Policy. (CVE-2016-9071)
- Multiple memory-corruption vulnerabilities. Successful exploits may allow an attacker to run arbitrary code. Failed exploit attempts could result in denial-of-service condition. (CVE-2016-5289) (CVE-2016-5290)
- A heap-buffer-overflow in the Cairo Graphics Library when processing Scalable Vector Graphics (SVG) content caused by compiler optimization. Specifically, this issue affects the 'rasterize_edges_1' function, and if exploited would cause denial-of-service condition or possible allow for arbitrary code execution. (CVE-2016-5296)
- A location bar spoofing vulnerability in Firefox for Android. (CVE-2016-9065)
- An information disclosure vulnerability exists in Mozilla Network Security Services (NSS) because it fails to properly handles Diffie Hellman Client keys. (CVE-2016-8635)

- A denial-of-service vulnerability exists in Mozilla Network Security Services (NSS) due to a Null-pointer dereference error. (CVE-2016-5285)

Mozilla Firefox ESR Vulnerabilities

- A security-bypass vulnerability. Specifically, this issue occurs because it is possible to write to arbitrary file with updater. An attacker can exploit this issue through the updater.log hardlink. (CVE-2016-5293)
- A security-bypass vulnerability. Specifically, this issue occurs because the updater can be made to choose an arbitrary target working directory for output files resulting from the update process. (CVE-2016-5294)
- A security-bypass vulnerability exists for Mozilla NSS. Specifically, this issue occurs due to insufficient timing side-channel resistance in 'divSpoiler'. (CVE-2016-9074)
- Multiple memory corruption vulnerabilities because it fails to properly verify argument length in JavaScript. Successful exploit result in integer overflows or other bounds checking issues. (CVE-2016-5297)
- A security-bypass vulnerability. Specifically, this issue occurs because the addon updates fails to properly verify that the add-on ID inside the signed package against the ID of the add-on being updated. (CVE-2016-9064)
- An integer-overflow vulnerability because it fails to properly bounds check user-supplied data before copying it into an insufficiently sized buffer. Specifically, this issue affects the 'nsScriptLoadHandler'. (CVE-2016-9066)
- A same-origin security-bypass vulnerability. An attacker can exploit this issue using local shortcut files to load arbitrary local content from disk. (CVE-2016-5291)

Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Customers whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

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.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

Mozilla:

<https://www.mozilla.org/en-US/security/advisories/mfsa2016-89/>

<https://www.mozilla.org/en-US/security/advisories/mfsa2016-90/>

<https://hg.mozilla.org/projects/nss/rev/45c047d18ac4>

Redhat:

https://bugzilla.redhat.com/show_bug.cgi?id=1391818

<https://rhn.redhat.com/errata/RHSA-2016-2779.html>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5285>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5289>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5290>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5291>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5292>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5293>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5294>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5295>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5296>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5297>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5298>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5299>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8635>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9061>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9062>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9063>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9064>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9065>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9066>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9067>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9068>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9069>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9070>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9071>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9072>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9073>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9074>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9075>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9076>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9077>

TLP: WHITE

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

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