

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:

04/27/2016

SUBJECT:

Multiple Vulnerabilities in Mozilla Firefox Could Allow for Arbitrary Code Execution

OVERVIEW:

Multiple vulnerabilities have been identified in Mozilla Firefox and Firefox ESR, the most severe of 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 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.

SYSTEMS AFFECTED:

- Mozilla Firefox versions prior to 46
- Mozilla Firefox ESR versions prior to 45.1 excluding 38.8

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 ESR. Exploitation of these vulnerabilities could allow for arbitrary code execution, security bypass, and access to sensitive data. 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:

- A denial-of-service vulnerability due to a null-pointer out-of-bounds read error (CVE-2016-2808)
- A heap based buffer-overflow vulnerability because it fails to properly bounds check user-supplied data before copying it into an insufficiently sized buffer. (CVE-2016-2814)
- Multiple memory-corruption vulnerabilities because it fails to adequately bounds-check user-supplied data. (CVE-2016-2807, CVE-2016-2806, CVE-2016-2805, CVE-2016-2804)
- A security-bypass vulnerability that affects the health reports. (CVE-2016-2820)

- A cross-site scripting vulnerability because it allows navigation to 'javascript:' URLs without additional permissions. (CVE-2016-2817)
- A cross-site scripting vulnerability. (CVE-2016-2816)
- An information-disclosure vulnerability affecting JavaScript with motion and orientation sensors. (CVE-2016-2813)
- A denial-of-service vulnerability due to an use-after free error. (CVE-2016-2811)
- A buffer-overflow vulnerability due to a race condition error. (CVE-2016-2812)
- A security-bypass vulnerability. Specifically, this issue occurs because the content providers protected with signature-level permissions can be accessed by an application. (CVE-2016-2810)
- A privilege-escalation vulnerability that affects the 'Maintenance Service' update. (CVE-2016-2809)

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:

<https://www.mozilla.org/en-US/security/advisories/mfsa2016-39>
<https://www.mozilla.org/en-US/security/advisories/mfsa2016-40>
<https://www.mozilla.org/en-US/security/advisories/mfsa2016-41>
<https://www.mozilla.org/en-US/security/advisories/mfsa2016-42>
<https://www.mozilla.org/en-US/security/advisories/mfsa2016-43>
<https://www.mozilla.org/en-US/security/advisories/mfsa2016-44>
<https://www.mozilla.org/en-US/security/advisories/mfsa2016-45>
<https://www.mozilla.org/en-US/security/advisories/mfsa2016-46>
<https://www.mozilla.org/en-US/security/advisories/mfsa2016-47>
<https://www.mozilla.org/en-US/security/advisories/mfsa2016-48>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2820>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2808>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2817>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2816>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2814>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2813>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2812>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2811>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2810>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2809>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2807>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2806>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2804>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2805>

TLP: WHITE

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

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