

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:

09/21/2016

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. Successful exploitation of these vulnerabilities could allow for arbitrary code execution, bypass security restrictions, perform unauthorized actions, or cause denial-of-service.

THREAT INTELLIGENCE:

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

SYSTEMS AFFECTED:

- Mozilla Firefox versions prior to 49
- Mozilla Firefox ESR versions prior to 45.4

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. Successful exploitation of these vulnerabilities could allow for arbitrary code execution, bypass security restrictions, perform unauthorized actions, or cause denial-of-service. 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 content security policy (CSP) containing a referrer directive with no values can cause a non-exploitable crash. (CVE-2016-2827)

- An out-of-bounds write of a boolean value during text conversion with some unicode characters. (CVE-2016-5270)
- An out-of-bounds read during the processing of text runs in some pages using display:contents. (CVE-2016-5271)
- A bad cast when processing layout with input elements can result in a potentially exploitable crash. (CVE-2016-5272)
- A potentially exploitable crash in accessibility. (CVE-2016-5273)
- A use-after-free vulnerability triggered by setting a aria-owns attribute. (CVE-2016-5276)
- A use-after-free issue in web animations during restyling. (CVE-2016-5274)
- A use-after-free vulnerability with web animations when destroying a timeline. (CVE-2016-5277)
- A buffer overflow when working with empty filters during canvas rendering. (CVE-2016-5275)
- A potentially exploitable crash caused by a buffer overflow while encoding image frames to images. (CVE-2016-5278)
- The full path to local files is available to scripts when local files are drag and dropped into Firefox. (CVE-2016-5279)
- Use-after-free vulnerability when changing text direction. (CVE-2016-5280)
- Use-after-free vulnerability when manipulating SVG format content through script. (CVE-2016-5281)
- Favicons can be loaded through non-whitelisted protocols, such as jar: (CVE-2016-5282)
- A timing attack vulnerability using iframes to potentially reveal private data using document resizes and link colors. (CVE-2016-5283)
- Mozilla developers Christoph Diehl, Christian Holler, Gary Kwong, Nathan Froyd, Honza Bambas, Seth Fowler, and Michael Smith reported memory safety bugs present in Firefox 48. Some of these bugs showed evidence of memory corruption under certain circumstances could potentially be exploited to run arbitrary code. (CVE-2016-5256)
- Due to flaws in the process we used to update "Preloaded Public Key Pinning" in our releases, the pinning for add-on updates became ineffective in early September. An attacker who was able to get a mis-issued certificate for a Mozilla web site could send malicious add-on updates to users on networks controlled by the attacker. Users who have not installed any add-ons are not affected. (CVE-2016-5284)
- URLs of resources loaded after a navigation started can leak to the following page through the Resource Timing API, leading to potential information disclosure. (CVE-2016-5250)
- An integer overflow error in WebSockets during data buffering on incoming packets resulting in attacker controlled data being written at a known offset in the allocated buffer. (CVE-2016-5261)
- Mozilla developers and community members Christoph Diehl, Andrew McCreight, Dan Minor, Byron Campen, Jon Coppeard, Steve Fink, Tyson Smith, Philipp, and Carsten Book reported memory safety bugs present in Firefox 48 and Firefox ESR 45.3. Some of these bugs showed evidence of memory corruption and we presume that with enough effort at least some of these could be exploited to run arbitrary code. (CVE-2016-5257)

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.

REFERENCES:

Mozilla:

<https://www.mozilla.org/en-US/security/advisories/mfsa2016-85/>

<https://www.mozilla.org/en-US/security/advisories/mfsa2016-86/>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2827>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5250>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5256>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5257>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5261>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5270>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5271>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5272>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5273>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5274>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5275>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5276>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5277>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5278>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5279>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5280>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5281>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5282>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5283>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5284>

TLP: WHITE

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

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