TLP: WHITE
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER:
2017-092

DATE(S) ISSUED:
09/29/2017

SUBJECT:
Multiple Vulnerabilities in Mozilla Firefox Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Mozilla Firefox and Firefox Extended Support Release (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. Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution. 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. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There is no evidence of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- Mozilla Firefox versions prior to 56
- Mozilla Firefox ESR versions prior to 52.4

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 the following vulnerabilities in Firefox and Firefox Extended Support Release (ESR).

- A use-after-free vulnerability can occur in the Fetch API when the worker or the associated window are freed when still in use, resulting in a potentially exploitable crash. (CVE-2017-7793)
- A spoofing vulnerability for Firefox for Android, that can occur when a page switches to fullscreen mode without user notification, allowing a fake address bar to be displayed. (CVE-2017-7817)
- A use-after-free vulnerability can occur when manipulating arrays of Accessible Rich Internet Applications (ARIA) elements within containers through the DOM. This results in a potentially exploitable crash. (CVE-2017-7818)
- A use-after-free vulnerability can occur in design mode when image objects are resized if objects referenced during the resizing have been freed from memory. This results in a potentially exploitable crash. (CVE-2017-7819)

- A buffer overflow occurs when drawing and validating elements with the ANGLE graphics library, used for WebGL content. This is due to an incorrect value being passed within the library during checks and results in a potentially exploitable crash. (CVE-2017-7824)
- Use-after-free vulnerability can occur in TLS 1.2 generating handshake hashes. During TLS 1.2 exchanges, handshake hashes are generated which point to a message buffer. This saved data is used for later messages but in some cases, the handshake transcript can exceed the space available in the current buffer, causing the allocation of a new buffer. This leaves a pointer pointing to the old, freed buffer, resulting in a use-after-free when handshake hashes are then calculated afterwards. This can result in a potentially exploitable crash. (CVE-2017-7805)
- Drag and drop of malicious page content to the tab bar can open locally stored files. If web content on a page is dragged onto portions of the browser UI, such as the tab bar, links can be opened that otherwise would not be allowed to open. This can allow malicious web content to open a locally stored file through ***file:*** URLs. (CVE-2017-7812)
- File downloads encoded with ***blob:*** and ***data:*** URL elements bypassed normal file download checks though the Phishing and Malware Protection feature and its block lists of suspicious sites and files, which could possibly allow malicious sites to have users download executables that would otherwise be detected as suspicious. (CVE-2017-7814)
- Inside the JavaScript parser, a cast of an integer to a narrower type can result in data read from outside the buffer being parsed. This usually results in a non-exploitable crash, but can leak a limited amount of information from memory if it matches JavaScript identifier syntax. (CVE-2017-7813)
- OS X fonts display some Tibetan and Arabic characters as whitespace, and if used as part of an IDN (internationalized domain name) in the address bar could be used for domain name spoofing attacks. Note: This attack only affects OS X operating systems. (CVE-2017-7825)
- On pages containing an iframe, the ***data:*** protocol can be used to create a modal dialog through Javascript that will have an arbitrary domains as the dialog's location, spoofing of the origin of the modal dialog from the user view. Note: This attack only affects installations with e10 multiprocess turned off. Installations with e10s turned on do not support the modal dialog functionality. (CVE-2017-7815)
- A vulnerability where WebExtensions could use popups and panels in the extension UI to load an ***about:*** privileged URL, violating security checks that disallow this behavior. (CVE-2017-7816)
- A vulnerability where WebExtensions can download and attempt to open a file of some non-executable file types. This can be triggered without specific user interaction for the file download and open actions. This could be used to trigger known vulnerabilities in the programs that handle those document types. (CVE-2017-7821)
- A Cross-Site Scripting (XSS) vulnerability exists, because the content security policy (CSP) ***sandbox*** directive does not create a unique origin for the document, causing it to behave as if the ***allow-same-origin*** keyword were always specified. (CVE-2017-7823)
- The AES-GCM implementation in WebCrypto API accepts 0-length IV when it should require a length of 1 according to the NIST Special Publication 800-38D specification. This might allow for the authentication key to be determined in some instances. (CVE-2017-7822)
- The *instanceof* operator can bypass the Xray wrapper mechanism. When called on web content from the browser itself or an extension the web content can provide its own result for that operator, possibly tricking the browser or extension into mishandling the element. (CVE-2017-7820)
- Multiple memory safety bugs have been reported —some of which showed evidence of memory corruption— that could be exploited to run arbitrary code. (CVE-2017-7810, CVE-2017-7811)

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution. 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. Users 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:
We recommend the following actions 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/mfsa2017-21/
https://www.mozilla.org/en-US/security/advisories/mfsa2017-22/

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7793
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7805
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7810
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7811
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7812
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7813
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7814
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7815
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7816
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7817
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7818
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7819
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7820
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7821
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7822
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7823
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7824
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7825

24×7 Security Operations Center
Multi-State Information Sharing and Analysis Center (MS-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722

MS-ISAC