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
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
05/21/2019

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

SYSTEMS AFFECTED:
- Mozilla Firefox versions prior to 67
- Mozilla Firefox ESR versions prior to 60.7

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:
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. Details of the vulnerabilities are as follows:

- A use-after-free vulnerability can occur when working with XMLHttpRequest (XHR) in an event loop, causing the XHR main thread to be called after it has been freed. This results in a potentially exploitable crash. (CVE-2019-11691)
- A malicious page can briefly cause the wrong name to be highlighted as the domain name in the address bar during page navigations. This could result in user confusion of which site is currently loaded for spoofing attacks. (CVE-2019-11699)
- An out-of-bounds read can occur in the Skia library during path transformations. This could result in the exposure of data stored in memory. (CVE-2019-5798)
- A possible vulnerability exists where type confusion can occur when manipulating JavaScript objects in object groups, allowing for the bypassing of security checks within these groups. Note: this vulnerability has only been demonstrated with UnboxedObjects, which are disabled by default on all supported releases. (CVE-2019-9816)
- A race condition is present in the crash generation server used to generate data for the crash reporter. This issue can lead to a use-after-free in the main process, resulting in a potentially exploitable crash and a sandbox escape. Note: this vulnerability only affects Windows. Other operating systems are unaffected. (CVE-2019-9818)
- A use-after-free vulnerability can occur when listeners are removed from the event listener manager while still in use, resulting in a potentially exploitable crash. (CVE-2019-11692)
- A custom cursor defined by scripting on a site can position itself over the addressbar to spoof the actual cursor when it should not be allowed outside of the primary web content area. This could be used by a malicious site to trick users into clicking on permission prompts, doorhanger notifications, or other buttons inadvertently if the location is spoofed over the user interface. (CVE-2019-11695)
- The default webcal: protocol handler will load a web site vulnerable to cross-site scripting (XSS) attacks. This default was left in place as a legacy feature and has now been removed. Note: this issue only affects users with an account on the vulnerable service. Other users are unaffected. (CVE-2019-11701)
- Memory safety bugs present in Firefox 66 and Firefox ESR 60.6. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. (CVE-2019-9800) (CVE-2019-9814)
- If hyperthreading is not disabled, a timing attack vulnerability exists, similar to previous Spectre attacks. Apple has shipped macOS 10.14.5 with an option to disable hyperthreading in applications running untrusted code in a thread through a new sysctl. Firefox now makes use of it on the main thread and any worker threads. Note: users need to update to macOS 10.14.5 in order to take advantage of this change. (CVE-2019-9815)
- A vulnerability exists in the Windows sandbox where an uninitialized value in memory can be leaked to a renderer from a broker when making a call to access an otherwise unavailable file. This results in the potential leaking of information stored at that memory location. Note: this issue only occurs on Windows. Other operating systems are unaffected. (CVE-2019-11694)
- A vulnerability where a JavaScript compartment mismatch can occur while working with the fetch API, resulting in a potentially exploitable crash. (CVE-2019-9819)
- A use-after-free vulnerability can occur in the chrome event handler when it is freed while still in use. This results in a potentially exploitable crash. (CVE-2019-9820)
- If the ALT and "a" keys are pressed when users receive an extension installation prompt, the extension will be installed without the install prompt delay that keeps the prompt visible in order for users to accept or decline the installation. A malicious web

page could use this with spoofing on the page to trick users into installing a malicious extension. (CVE-2019-11697)

- A hyperlink using the res: protocol can be used to open local files at a known location in Internet Explorer if a user approves execution when prompted. Note: this issue only occurs on Windows. Other operating systems are unaffected. (CVE-2019-11700)
- Cross-origin images can be read from a canvas element in violation of the same-origin policy using the transferFromImageBitmap method. Note: This only affects Firefox 65. Previous versions are unaffected. (CVE-2018-18511)
- If a crafted hyperlink is dragged and dropped to the bookmark bar or sidebar and the resulting bookmark is subsequently dragged and dropped into the web content area, an arbitrary query of a user's browser history can be run and transmitted to the content page via drop event data. This allows for the theft of browser history by a malicious site. (CVE-2019-11698)
- Cross-origin images can be read in violation of the same-origin policy by exporting an image after using createImageBitmap to read the image and then rendering the resulting bitmap image within a canvas element. (CVE-2019-9797)
- Images from a different domain can be read using a canvas object in some circumstances. This could be used to steal image data from a different site in violation of same-origin policy. (CVE-2019-9817)
- Files with the .JNLP extension used for "Java web start" applications are not treated as executable content for download prompts even though they can be executed if Java is installed on the local system. This could allow users to mistakenly launch an executable binary locally. (CVE-2019-11696)
- A use-after-free vulnerability can occur in AssertWorkerThread due to a race condition with shared workers. This results in a potentially exploitable crash. (CVE-2019-9821)
- A use-after-free vulnerability was discovered in the png_image_free function in the libpng library. This could lead to denial of service or a potentially exploitable crash when a malformed image is processed. (CVE-2019-7317)
- The bufferdata function in WebGL is vulnerable to a buffer overflow with specific graphics drivers on Linux. This could result in malicious content freezing a tab or triggering a potentially exploitable crash. Note: this issue only occurs on Linux. Other operating systems are unaffected. (CVE-2019-11693)

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:

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/mfsa2019-13/
https://www.mozilla.org/en-US/security/advisories/mfsa2019-14/

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18511
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5798
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7317
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9797
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9800
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9814
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9815
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9816
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9817
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9818
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9819
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9820
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9821
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11691
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11692
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11693
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11694
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11695
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11696
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11697
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11698
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11699
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11700
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11701

Greg Nohra
Enterprise Security Architect
MS Department of Information Technology Services
601-432-8009 | www.its.ms.gov