TLP: WHITE
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER: 2018-072

DATE(S) ISSUED: 06/27/2018

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 61
- Mozilla Firefox ESR versions prior to 60.1
- Mozilla Firefox ESR versions prior to 52.9

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 buffer overflow can occur when rendering canvas content while adjusting the height and width of the <canvas> element dynamically, causing data to be written outside of the currently computed boundaries. This results in a potentially exploitable crash. (CVE-2018-12359)
- A compromised IPC child process can escape the content sandbox and list the names of arbitrary files on the file system without user consent or interaction. This could result in exposure of private local files. (CVE-2018-12365)
- An integer overflow can occur during graphics operations done by the Supplemental Streaming SIMD Extensions 3 (SSSE3) scaler, resulting in a potentially exploitable crash. (CVE-2018-12362)
- An integer overflow can occur in the SwizzleData code while calculating buffer sizes. The overflowed value is used for subsequent graphics computations when their inputs are not sanitized which results in a potentially exploitable crash. (CVE-2018-12361)
- An integer overflow vulnerability in the Skia library when allocating memory for edge builders on some systems with at least 16 GB of RAM. This results in the use of uninitialized memory, resulting in a potentially exploitable crash. (CVE-2018-12371)

- An invalid grid size during QCMS (color profile) transformations can result in the out-of-bounds read interpreted as a float value. This could leak private data into the output. (CVE-2018-12366)
- A use-after-free vulnerability can occur when deleting an input element during a mutation event handler triggered by focusing that element. This results in a potentially exploitable crash. (CVE-2018-12360)
- A use-after-free vulnerability can occur when script uses mutation events to move DOM nodes between documents, resulting in the old document that held the node being freed but the node still having a pointer referencing it. This results in a potentially exploitable crash. (CVE-2018-12363)
- A vulnerability can occur when capturing a media stream when the media source type is changed as the capture is occuring. This can result in stream data being cast to the wrong type causing a potentially exploitable crash. (CVE-2018-5156)
- Some reported memory safety bugs present in Firefox 60, Firefox ESR 60, and Firefox ESR 52.8 showed evidence of memory corruption and it is believed that these could be exploited to run arbitrary code. (CVE-2018-5188)
- Some reported memory safety bugs present in Firefox 60 showed evidence of memory corruption and it is believed that these could be exploited to run arbitrary code. (CVE-2018-5186)
- Some reported memory safety bugs present in Firefox 60 and Firefox ESR 60 showed evidence of memory corruption and it is believed that these could be exploited to run arbitrary code. (CVE-2018-5187)
- In Reader View SameSite cookie protections are not checked on exiting. This allows for a payload to be triggered when Reader View is exited if loaded by a malicious site while Reader mode is active, bypassing CSRF protections. (CVE-2018-12370)
- In the previous mitigations for Spectre, the resolution or precision of various methods was reduced to counteract the ability to measure precise time intervals. In that work, PerformanceNavigationTiming was not adjusted but it was found that it could be used as a precision timer. (CVE-2018-12367)
- NPAPI plugins, such as Adobe Flash, can send non-simple cross-origin requests, bypassing CORS by making a same-origin POST that does a 307 redirect to the target site. This allows for a malicious site to engage in cross-site request forgery (CSRF) attacks. (CVE-2018-12364)
- Service workers can use redirection to avoid the tainting of cross-origin resources in some instances, allowing a malicious site to read responses which are supposed to be opaque. (CVE-2018-12358)
- WebExtensions bundled with embedded experiments were not correctly checked for proper authorization. This allowed a malicious WebExtension to gain full browser permissions. (CVE-2018-12369)
- Windows 10 does not warn users before opening executable files with the SettingContent-ms extension even when they have been downloaded from the internet and have the "Mark of the Web." Without the warning, unsuspecting users unfamiliar with this new file type might run an unwanted executable. This also allows a WebExtension with the limited downloads.open permission to execute arbitrary code without user interaction on Windows 10 systems. Note: this issue only affects Windows operating systems. Other operating systems are unaffected. (CVE-2018-12368)

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution. Depending on the privileges associated with the user group, 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/mfsa2018-15/
https://www.mozilla.org/en-US/security/advisories/mfsa2018-16/
https://www.mozilla.org/en-US/security/advisories/mfsa2018-17/

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5156
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5186
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5187
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5188
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12358
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12359
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12360
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12361
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12362
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12363
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12364
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12365
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12366
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12367
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12368
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12369
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12370
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12371

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

MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

Elections
Infrastructure
ISAC

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/