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
https://www.cisa.gov/tlp
Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

DATE(S) ISSUED:
06/02/2021

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

OVERVIEW:
Multiple vulnerabilities have been discovered in Mozilla Firefox, Firefox Extended Support Release (ESR) and Mozilla Firefox for iOS, 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. Mozilla Firefox for iOS is a web browser used to access the Internet on Apple Products. Successful exploitation 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 89
- Firefox ESR versions prior to 78.11
- Firefox for iOS versions prior to 34

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Mozilla Firefox, and Firefox Extended Support Release (ESR), and Mozilla Firefox for iOS, the most severe of which could allow for arbitrary code execution. Details of these vulnerabilities are as follows:

- File download shares private browsing mode cookies. (CVE-2021-29958)
- When a user has already allowed a website to access microphone and camera, disabling camera sharing would not fully prevent the website from re-enabling it without an additional prompt. This was only possible if the website kept recording with the microphone until re-enabling the camera. (CVE-2021-29959)
- Firefox used to cache the last filename used for printing a file. When generating a filename for printing, Firefox usually suggests the web page title. The caching and suggestion techniques combined may have led to the title of a website visited during private browsing mode being stored on disk. (CVE-2021-29960)
- When styling and rendering an oversized <select> element, Firefox did not apply correct clipping which allowed an attacker to paint over the user interface. (CVE-2021-29961)
- Firefox for Android would become unstable and hard-to-recover when a website opened too many popups. NOTE: This bug only affects Firefox for Android. Other operating systems are unaffected. (CVE-2021-29962)
- Address bar search suggestions in private browsing mode were re-using session data from normal mode. NOTE: This bug only affects Firefox for Android. Other operating systems are unaffected. (CVE-2021-29963)
- A locally-installed hostile program could send WM_COPYDATA messages that Firefox would process incorrectly, leading to an out-of-bounds read. NOTE: This bug only affects Firefox on Windows. Other operating systems are unaffected. (CVE-2021-29964)
- A malicious website that causes an HTTP Authentication dialog to be spawned could trick the built-in password manager to suggest passwords for the currently active website instead of the website that triggered the dialog. NOTE: This bug only affects Firefox for Android. Other operating systems are unaffected. (CVE-2021-29965)
- Mozilla developers Christian Holler, Tooru Fujisawa, Tyson Smith reported memory safety bugs present in Firefox 88. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2021-29966)
- Mozilla developers Christian Holler, Anny Gakhokidze, Alexandru Michis, Gabriele Svelto reported memory safety bugs present in Firefox 88 and Firefox ESR 78.11. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2021-29967)

Successful exploitation 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/mfsa2021-23/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-24/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-25/

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29958
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29959
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29960
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29961
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29962
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29963
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29964
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29965
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29966
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29967

TLP: WHITE
https://www.cisa.gov/tlp
Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.