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:
08/10/2021

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 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 91
- Firefox ESR versions prior to 78.13

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), the most severe of which could allow for arbitrary code execution. Details of these vulnerabilities are as follows:

- A suspected race condition when calling getaddrinfo led to memory corruption and a potentially exploitable crash (CVE-2021-29986) *Note: This issue only affected Linux operating systems. Other operating systems are unaffected.*
- An issue present in lowering/register allocation could have led to obscure but deterministic register confusion failures in JITted code that would lead to a potentially exploitable crash (CVE-2021-29981).
- Firefox incorrectly treated an inline list-item element as a block element, resulting in an out of bounds read or memory corruption, and a potentially exploitable crash (CVE-2021-29988).
- Firefox for Android could get stuck in fullscreen mode and not exit it even after normal interactions that should cause it to exit (CVE-2021-29983) *Note: This issue only affected Firefox for Android. Other operating systems are unaffected.*
- Instruction reordering resulted in a sequence of instructions that would cause an object to be incorrectly considered during garbage collection. This led to memory corruption and a potentially exploitable crash (CVE-2021-29984).
- Uninitialized memory in a canvas object could have caused an incorrect free() leading to memory corruption and a potentially exploitable crash (CVE-2021-29980).
- After requesting multiple permissions, and closing the first permission panel, subsequent permission panels will be displayed in a different position but still record a click in the default location, making it possible to trick a user into accepting a permission they did not want to (CVE-2021-29987) *This bug only affects Firefox on Linux. Other operating systems are unaffected.*
- A use-after-free vulnerability in media channels could have led to memory corruption and a potentially exploitable crash (CVE-2021-29985).
- Due to incorrect JIT optimization, we incorrectly interpreted data from the wrong type of object, resulting in the potential leak of a single bit of memory (CVE-2021-29982).
- Memory safety bugs are present in Firefox 90 and Firefox ESR 78.12. Some of these bugs showed evidence of memory corruption and are presumed that with enough effort some of these could have been exploited to run arbitrary code (CVE-2021-29989).
- Memory safety bugs are present in Firefox 90. Some of these bugs showed evidence of memory corruption and are presumed that with enough effort some of these could have been exploited to run arbitrary code (CVE-2021-29990).

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/mfsa2021-33/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-34/

CVE:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29980
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29981
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29982
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29983
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29984
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29985
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29986
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29987
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29988
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29989
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29990

TLP: WHITE

https://www.cisa.gov/tlp