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:
07/13/2021

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 90
- Firefox ESR versions prior to 78.12

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 malicious webpage could have triggered a use-after-free, memory corruption, and a potentially exploitable crash. NOTE: This bug only affected Firefox when accessibility was enabled. (CVE-2021-29970)
- If a user had granted a permission to a webpage and saved that grant, any webpage running on the same host - irrespective of scheme or port - would be granted that permission. NOTE: This bug only affects Firefox for Android. Other operating systems are unaffected. (CVE-2021-29971)
- A user-after-free vulnerability was found via testing, and traced to an out-of-date Cairo library. Updating the library resolved the issue, and may have remediated other, unknown security vulnerabilities as well. (CVE-2021-29972)
- Password autofill was enabled without user interaction on insecure websites on Firefox for Android. This was corrected to require user interaction with the page before a user's password would be entered by the browser's autofill functionality. NOTE: This bug only affects Firefox for Android. Other operating systems are unaffected. (CVE-2021-29973)
- When network partitioning was enabled, e.g. as a result of Enhanced Tracking Protection settings, a TLS error page would allow the user to override an error on a domain which had specified HTTP Strict Transport Security (which implies that the error should not be override-able.) This issue did not affect the network connections, and they were correctly upgraded to HTTPS automatically. (CVE-2021-29974)
- Through a series of DOM manipulations, a message, over which the attacker had control of the text but not HTML or formatting, could be overlaid on top of another domain (with the new domain correctly shown in the address bar) resulting in possible user confusion. (CVE-2021-29975)
- Memory safety bugs fixed in Firefox 89 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-2021-29976)
- Memory safety bugs fixed in Firefox 89. 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-2021-29977)
- An out of bounds write in ANGLE could have allowed an attacker to corrupt memory leading to a potentially exploitable crash. (CVE-2021-30547)

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/mfsa2021-28/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-29/

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29970
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29971
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29972
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29973
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29974
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29975
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29976
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29977
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30547

TLP: WHITE
https://www.cisa.gov/tlp