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:
12/08/2021

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

OVERVIEW:
Multiple vulnerabilities have been discovered in Mozilla Firefox, Firefox Extended Support Release (ESR), and Thunderbird, 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 Thunderbird is an email client. 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 95
- Firefox ESR versions prior to 91.4
- Thunderbird versions prior to 91.4

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, Firefox Extended Support Release (ESR), and Thunderbird, the most severe of which could allow for arbitrary code execution. Details of these vulnerabilities are as follows:

- JavaScript unexpectedly enabled for the composition area (CVE-2021-43528)
- URL leakage when navigating while executing asynchronous function (CVE-2021-43536)
- Heap buffer overflow when using structured clone (CVE-2021-43537)
- Missing fullscreen and pointer lock notification when requesting both (CVE-2021-43538)
- GC rooting failure when calling wasm instance methods (CVE-2021-43539)
- WebExtensions could have installed persistent ServiceWorkers (CVE-2021-43540)
- External protocol handler parameters were unescaped (CVE-2021-43541)
- XMLHttpRequest error codes could have leaked the existence of an external protocol handler (CVE-2021-43542)
- Bypass of CSP sandbox directive when embedding (CVE-2021-43543)
- Receiving a malicious URL as text through a SEND intent could have led to XSS (CVE-2021-43544)
- Denial of Service when using the Location API in a loop (CVE-2021-43545)
- Cursor spoofing could overlay user interface when native cursor is zoomed (CVE-2021-43546)

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/mfsa2021-52/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-53/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-54/

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43528
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43536
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43537
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43538
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43539
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43540
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43541
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43542

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43543
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43544
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43545
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43546

TLP: WHITE

https://www.cisa.gov/tlp