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
www.cisa.gov/tlp
Information may be distributed without restriction, subject to standard copyright rules.

DATE(S) ISSUED:
06/01/2022

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

OVERVIEW:
Multiple vulnerabilities have been discovered in Mozilla Firefox, Firefox Extended Support Release (ESR) and Mozilla 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

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- Mozilla Firefox versions prior to 101
- Firefox ESR versions prior to 91.10
- Thunderbird versions prior to 91.10

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

Tactic: *Execution* **(**TA0002**)**:

- CVE-2022-31737: Heap buffer overflow in WebGL
- CVE-2022-1919: Memory Corruption when manipulating webp images
- CVE-2022-31747: Memory safety bugs fixed in Firefox 101 and Firefox ESR 91.10
- CVE-2022-31748: Memory safety bugs fixed in Firefox 101
- CVE-2022-31740: Register allocation problem in WASM on arm64
- CVE-2022-31741: Uninitialized variable leads to invalid memory read

Additional vulnerabilities include:

- CVE-2022-31736: Cross-Origin resource's length leaked
- CVE-2022-31738: Browser window spoof using fullscreen mode
- CVE-2022-31739: Attacker-influenced path traversal when saving downloaded files
- CVE-2022-31742: Querying a WebAuthn token with a large number of allowCredential entries may have leaked cross-origin information
- CVE-2022-31743: HTML Parsing incorrectly ended HTML comments prematurely
- CVE-2022-31744: CSP bypass enabling stylesheet injection
- CVE-2022-31745: Incorrect Assertion caused by unoptimized array shift operations
- CVE-2022-1834: Braille space character caused incorrect sender email to be shown for a digitally signed email

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:
We recommend the following actions be taken:

- Apply appropriate updates provided by Mozilla to vulnerable systems immediately after appropriate testing. (**M1051: Update Software**)
    - **Safeguard 7.1: Establish and Maintain a Vulnerability Management Process**: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 7.4: Perform Automated Application Patch Management:** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
- Apply the Principle of Least Privilege to all systems and services. Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack. . (**M1026: Privileged Account Management**)
    - **Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software:** Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.
    - **Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts:** Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources. Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources. (**M1017: User Training**)
    - **Safeguard 14.1: Establish and Maintain a Security Awareness Program:** Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 14.2: Train Workforce Members to Recognize Social Engineering Attacks:** Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.

REFERENCES:

Mozilla:

https://www.mozilla.org/en-US/security/advisories/mfsa2022-20/

https://www.mozilla.org/en-US/security/advisories/mfsa2022-21/

https://www.mozilla.org/en-US/security/advisories/mfsa2022-22/

CISA:

https://www.cisa.gov/uscert/ncas/current-activity/2022/06/01/mozilla-releases-security-updates-firefox-firefox-esr-and

CVE:

https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1834

https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1919

https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31736

https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31737

https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31738

https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31739

https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31740

https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31741

https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31742

https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31743

https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31744

https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31745

https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31747

https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31748