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:
01/11/2022

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 96
- Firefox ESR versions prior to 91.5
- Thunderbird versions prior to 91.5

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:

- Iframe sandbox bypass with XSLT (CVE-2021-4140)
- Potential local privilege escalation when loading modules from the install directory. (CVE-2022-22736)
- Race condition when playing audio files (CVE-2022-22737)
- Heap-buffer-overflow in blendGaussianBlur (CVE-2022-22738)
- Missing throttling on external protocol launch dialog (CVE-2022-22739)
- Use-after-free of ChannelEventQueue::mOwner (CVE-2022-22740)
- Browser window spoof using fullscreen mode (CVE-2022-22741)
- Out-of-bounds memory access when inserting text in edit mode (CVE-2022-22742)
- Browser window spoof using fullscreen mode (CVE-2022-22743)
- The 'Copy as curl' feature in DevTools did not fully escape website-controlled data, potentially leading to command injection (CVE-2022-22744)
- Leaking cross-origin URLs through securitypolicyviolation event (CVE-2022-22745)
- Calling into reportValidity could lead to fullscreen window spoof (CVE-2022-22746)
- Crash when handling empty pkcs7 sequence (CVE-2022-22747)
- Spoofed origin on external protocol launch dialog (CVE-2022-22748)
- Lack of URL restrictions when scanning QR codes (CVE-2022-22749)
- IPC passing of resource handles could lead to sandbox bypass (CVE-2022-22750)
- Memory safety bugs fixed in Firefox 95, Firefox ESR 91.4, and Thunderbird 91.4 (CVE-2022-22751)
- Memory safety bugs fixed in Firefox 95 (CVE-2022-22752)

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/mfsa2022-01/

https://www.mozilla.org/en-US/security/advisories/mfsa2022-02/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-03/

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4140
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22736
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22737
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22738
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22739
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22740
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22741
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22742
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22743
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22744
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22745
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22746
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22747
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22748
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22749
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22750
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22751
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22752

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.