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
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
02/24/2021

SUBJECT:
Multiple Vulnerabilities in Mozilla Firefox and Thunderbird 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 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 reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:

- Mozilla Firefox versions prior to 86
- Firefox ESR versions prior to 78.8
- Mozilla Thunderbird versions prior to 78.8

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, and 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:

- As specified in the W3C Content Security Policy draft, when creating a violation report, "User agents need to ensure that the source file is the URL requested by the page, pre-redirects. If that’s not possible, user agents need to strip the URL down to an origin to avoid unintentional leakage." Under certain types of redirects, Firefox incorrectly set the source file to be the destination of the redirects. This was fixed to be the redirect destination's origin. [CVE-2021-23969]
- Context-specific code was included in a shared jump table; resulting in assertions being triggered in multithreaded wasm code. [CVE-2021-23970]
- If Content Security Policy blocked frame navigation, the full destination of a redirect served in the frame was reported in the violation report; as opposed to the original frame URI. This could be used to leak sensitive information contained in such URIs. [CVE-2021-23968]
- The DOMParser API did not properly process <noscript> elements for escaping. This could be used as an mXSS vector to bypass an HTML Sanitizer. [CVE-2021-23974]
- When processing a redirect with a conflicting Referrer-Policy, Firefox would have adopted the redirect's Referrer-Policy. This would have potentially resulted in more information than intended by the original origin being provided to the destination of the redirect. [CVE-2021-23971]
- When accepting a malicious intent from other installed apps, Firefox for Android accepted manifests from arbitrary file paths and allowed declaring webapp manifests for other origins. This could be used to gain fullscreen access for UI spoofing and could also lead to cross-origin attacks on targeted websites.
- Note: This issue is a different issue from CVE-2020-26954 and only affected Firefox for Android. Other operating systems are unaffected. [CVE-2021-23976]
- Firefox for Android suffered from a time-of-check-time-of-use vulnerability that allowed a malicious application to read sensitive data from application directories.
- Note: This issue is only affected Firefox for Android. Other operating systems are unaffected. [CVE-2021-23977]
- One phishing tactic on the web is to provide a link with HTTP Auth. For example https://www.phishingtarget.com@evil.com. To mitigate this type of attack, Firefox will display a warning dialog; however, this warning dialog would not have been displayed if evil.com used a redirect that was cached by the browser. [CVE-2021-23972]
- The developer page about:memory has a Measure function for exploring what object types the browser has allocated and their sizes. When this function was invoked we incorrectly called the sizeof function, instead of using the API method that checks for invalid pointers. [CVE-2021-23975]
- When trying to load a cross-origin resource in an audio/video context a decoding error may have resulted, and the content of that error may have revealed information about the resource. [CVE-2021-23973]
- Mozilla developers Alexis Beingessner, Tyson Smith, Nika Layzell, and Mats Palmgren reported memory safety bugs present in Firefox 85 and Firefox ESR 78.7. 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-2021-23978]
- Mozilla developers Tyson Smith, Lars T Hansen, Valentin Gosu, and Sebastian Hengst reported memory safety bugs present in Firefox 85. 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-2021-23979]

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/mfsa2021-07/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-08/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-09/

CVE:

https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2021-23968
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2021-23969
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2021-23970
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2021-23971
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2021-23972
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2021-23973
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2021-23974
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2021-23975
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2021-23976
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2021-23977
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2021-23978
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2021-23979