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:
01/27/2021

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 no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- Mozilla Firefox versions prior to 85
- Mozilla Firefox ESR versions prior to 78.7
- Mozilla Thunderbird versions prior to 78.7

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:

- During the plaintext phase of the STARTTLS connection setup, protocol commands could have been injected and evaluated within the encrypted session. [CVE-2020-15685]
- When a HTTPS page was embedded in a HTTP page, and there was a service worker registered for the former, the service worker could have intercepted the request for the secure page despite the iframe not being a secure context due to the (insecure) framing. [CVE-2020-26976]
- If a user clicked into a specifically crafted PDF, the PDF reader could be confused into leaking cross-origin information, when said information is served as chunked data. [CVE-2021-23953]
- Using the new logical assignment operators in a JavaScript switch statement could have caused a type confusion, leading to a memory corruption and a potentially exploitable crash. [CVE-2021-23954]
- The browser could have been confused into transferring a pointer lock state into another tab, which could have lead to clickjacking attacks. [CVE-2021-23955]
- An ambiguous file picker design could have confused users who intended to select and upload a single file into uploading a whole directory. This was addressed by adding a new prompt. [CVE-2021-23956]
- Navigations through the Android-specific intent URL scheme could have been misused to escape iframe sandbox. Note: This issue only affected Firefox for Android. Other operating systems are unaffected. [CVE-2021-23957]
- The browser could have been confused into transferring a screen sharing state into another tab, which would leak unintended information. [CVE-2021-23958]
- An XSS bug in internal error pages could have led to various spoofing attacks, including other error pages and the address bar.Note: This issue only affected Firefox for Android. Other operating systems are unaffected [CVE-2021-23959]
- Performing garbage collection on re-declared JavaScript variables resulted in a user-after-poison, and a potentially exploitable crash. [CVE-2021-23960]
- Further techniques that built on the slipstream research combined with a malicious webpage could have exposed both an internal network's hosts as well as services running on the user's local machine. [CVE-2021-23961]
- Incorrect use of the RowCountChanged method could have led to a user-after-poison and a potentially exploitable crash. [CVE-2021-23962]
- When sharing geolocation during an active WebRTC share, Firefox could have reset the webRTC sharing state in the user interface, leading to loss of control over the currently granted permission [CVE-2021-23963]
- A security vulnerability that occurs due to memory safety bugs. [CVE-2021-23964, CVE-2021-23965]

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/mfsa2021-05/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-04/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-03/

CVE:

https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2020-15685
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2020-26976
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2021-23953
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2021-23954
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2021-23955
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2021-23956
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2021-23957
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2021-23958
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2021-23959
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2021-23960
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2021-23961
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2021-23962
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2021-23963
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2021-23964
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2021-23965