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:
03/24/2021

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 no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- Mozilla Firefox versions prior to 87
- Firefox ESR versions prior to 78.9
- Mozilla Thunderbird versions prior to 78.9

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

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:

- A texture upload of a Pixel Buffer Object could have confused the WebGL code to skip binding the buffer used to unpack it, resulting in memory corruption and a potentially exploitable information leak or crash (CVE-2021-23981).
- Using techniques that built on the slipstream research, a malicious webpage could have scanned both an internal network's hosts as well as services running on the user's local machine utilizing WebRTC connections (CVE-2021-23982).
- By causing a transition on a parent node by removing a CSS rule, an invalid property for a marker could have been applied, resulting in memory corruption and a potentially exploitable crash (CVE-2021-23983).
- A malicious extension could have opened a popup window lacking an address bar. The title of the popup lacking an address bar should not be fully controllable, but in this situation was. This could have been used to spoof a website and attempt to trick the user into providing credentials (CVE-2021-23984).
- If an attacker is able to alter specific about:config values (for example malware running on the user's computer), the Devtools remote debugging feature could have been enabled in a way that was unnoticable to the user. This would have allowed a remote attacker (able to make a direct network connection to the victim) to monitor the user's browsing activity and (plaintext) network traffic. This was addressed by providing a visual cue when Devtools has an open network socket (CVE-2021-23985).
- A malicious extension with the 'search' permission could have installed a new search engine whose favicon referenced a cross-origin URL. The response to this cross-origin request could have been read by the extension, allowing a same-origin policy bypass by the extension, which should not have cross-origin permissions. This cross-origin request was made without cookies, so the sensitive information disclosed by the violation was limited to local-network resources or resources that perform IP-based authentication (CVE-2021-23986).
- Mozilla developers and community members Matthew Gregan, Tyson Smith, Julien Wajsberg, and Alexis Beingessner reported memory safety bugs present in Firefox 86 and Firefox ESR 78.8. 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-2021-23987).
- Mozilla developers Tyson Smith and Christian Holler reported memory safety bugs present in Firefox 86. 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-2021-23988).

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/mfsa2021-10/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-11/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-12/

CVE:

https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2021-23981
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2021-23982
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2021-23983
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2021-23984
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2021-23985
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2021-23986
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2021-23987
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2021-23988

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.