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:
11/03/2021

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

OVERVIEW:
Multiple vulnerabilities have been discovered in Mozilla Firefox and Firefox Extended Support Release (ESR), 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. 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 94
- Firefox ESR versions prior to 91.3

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

- Iframe sandbox rules did not apply to XSLT stylesheets (CVE-2021-38503)

- Use-after-free in file picker dialog (CVE-2021-38504)
- Windows 10 Cloud Clipboard may have recorded sensitive user data (CVE-2021-38505)
- Firefox could be coaxed into going into fullscreen mode without notification or warning (CVE-2021-38506)
- Opportunistic Encryption in HTTP2 could be used to bypass the Same-Origin-Policy on services hosted on other ports (CVE-2021-38507)
- Improper sanitization when processing a QR code resulted in Universal XSS (MOZ-2021-0003)
- Permission Prompt could be overlaid, resulting in user confusion and potential spoofing (CVE-2021-38508)
- Web Extensions could access pre-redirect URL when their context menu was triggered by a user (MOZ-2021-0004)
- Javascript alert box could have been spoofed onto an arbitrary domain (CVE-2021-38509)
- Download Protections were bypassed by .inetloc files on Mac OS (CVE-2021-38510)
- 'Copy Image Link' context menu action could have been abused to see authentication tokens (MOZ-2021-0005)
- URL Parsing may incorrectly parse internationalized domains (MOZ-2021-0006)
- Memory safety bugs in Firefox 93 and Firefox ESR 91.2 could result in arbitrary code execution (MOZ-2021-0007)
- Use-after-free in HTTP2 Session object may cause exploitable crashes (MOZ-2021-0008)

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/mfsa2021-48/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-49/

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38503
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38504
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38505

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38506
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38507
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38508
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38509
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38510

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.