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
www.cisa.gov/tlp
Information may be distributed without restriction, subject to standard copyright rules.

DATE(S) ISSUED:
05/04/2022

SUBJECT:
Multiple Vulnerabilities in Firefox Products 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 99
- Firefox ESR versions prior to 91.8

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

- Fullscreen notification bypass using popups (CVE-2022-29914)
- Bypassing permission prompt in nested browsing contexts (CVE-2022-29909)
- Leaking browser history with CSS variables (CVE-2022-29916)
- Reader mode bypassed SameSite cookies (CVE-2022-29912)
- Firefox for Android forgot HTTP Strict Transport Security settings (CVE-2022-29910)
- Leaking cross-origin redirect through the Performance API (CVE-2022-29915)
- iframe Sandbox bypass (CVE-2022-29911)
- Memory safety bugs fixed in Firefox 100 and Firefox ESR 91.9 (CVE-2022-29917)
- Memory safety bugs fixed in Firefox 100 (CVE-2022-29918)

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:

We recommend the following actions 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/mfsa2022-16/
https://www.mozilla.org/en-US/security/advisories/mfsa2022-17/

CISA:

https://www.cisa.gov/uscert/ncas/current-activity/2022/05/04/mozilla-releases-security-updates-firefox-and-firefox-esr

CVE:

https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29914
https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29909
https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29916
https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29912
https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29910
https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29915
https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29911
https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29917
https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29918