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:
10/20/2022

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

OVERVIEW:
Multiple vulnerabilities have been discovered in Mozilla Firefox and Firefox 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 in the context of the logged on user. 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 106
- Firefox ESR versions prior to 102.4

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

Tactic: *Initial Access* (TA0001):

Technique: *Drive-by Compromise* (T1189):

- CVE-2022-42928: Memory Corruption in JS Engine
- CVE-2022-42932: Memory safety bugs fixed in Firefox 106 and Firefox ESR 102.4

Details of lower-severity vulnerabilities are as follows:

- CVE-2022-42927: Same-origin policy violation could have leaked cross-origin URLs
- CVE-2022-42929: Denial of Service via window.print
- CVE-2022-42930: Race condition in DOM Workers
- CVE-2022-42931: Username saved to a plaintext file on disk

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution in the context of the logged on user. 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. (**M1051: Update Software**)
  - **Safeguard 7.1: Establish and Maintain a Vulnerability Management Process**: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
  - **Safeguard 7.2: Establish and Maintain a Remediation Process**: Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.
  - **Safeguard 7.4: Perform Automated Application Patch Management:** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.

    - **Safeguard 7.5: Perform Automated Vulnerability Scans of Internal Enterprise Assets:** Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.
    - **Safeguard 9.1: Ensure Use of Only Fully Supported Browsers and Email Clients:** Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.
- Apply the Principle of Least Privilege to all systems and services. Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack. (**M1026: Privileged Account Management**)
    - **Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software:** Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.
    - **Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts:** Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user’s primary, non-privileged account.

- Restrict execution of code to a virtual environment on or in transit to an endpoint system. (**M1048: Application Isolation and Sandboxing**)

- Restrict use of certain websites, block downloads/attachments, block Javascript, restrict browser extensions, etc. (**M1021: Restrict Web-Based Content**)
    - **Safeguard 2.3: Address Unauthorized Software:** Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.
    - **Safeguard 2.7: Allowlist Authorized Scripts:** Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassessbi-annually, or more frequently.
    - **Safeguard 9.3: Maintain and Enforce Network-Based URL Filters:** Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.
    - **Safeguard 9.6: Block Unnecessary File Types:** Block unnecessary file types attempting to enter the enterprise’s email gateway.

- Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring. (**M1050: Exploit Protection**)
    - **Safeguard 10.5: Enable Anti-Exploitation Features:** Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG),

or Apple® System Integrity Protection (SIP) and Gatekeeper™.

- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources. Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources. (**M1017: User Training**)
  - **Safeguard 14.1: Establish and Maintain a Security Awareness Program:** Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.
  - **Safeguard 14.2: Train Workforce Members to Recognize Social Engineering Attacks:** Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.

REFERENCES:

Mozilla:

https://www.mozilla.org/en-US/security/advisories/mfsa2022-44/

https://www.mozilla.org/en-US/security/advisories/mfsa2022-45/

CVE:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-42927

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-42928

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-42929

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-42930

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-42931

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-42932