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:
06/29/2022

SUBJECT:
Multiple Vulnerabilities in Mozilla Products 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 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 102
- Firefox ESR versions prior to 91.11
- Thunderbird versions prior to 91.11

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:

Tactic: *Execution* (TA0002):

Technique: *Exploitation for Client Execution* (T1203)

- CVE-2022-34484: Memory safety bugs fixed in Firefox 102 and Firefox ESR 91.11

Technique: *User Executio*n (T1204)

- CVE-2022-34482: Drag and drop of malicious image could have led to malicious executable and potential code execution
- CVE-2022-34483: Drag and drop of malicious image could have led to malicious executable and potential code execution
- CVE-2022-34468: CSP sandbox header without `allow-scripts` can be bypassed via retargeted javascript: URI

Tactic: *Impact* (TA0040):

Technique: *Endpoint Denial of Service: Application or System Exploitation* (T1499.004)

- CVE-2022-34470: Use-after-free in nsSHistory

Additional vulnerabilities include:

- CVE-2022-34476: ASN.1 parser could have been tricked into accepting malformed ASN.1
- CVE-2022-34481: Potential integer overflow in ReplaceElementsAt
- CVE-2022-34474: Sandboxed iframes could redirect to external schemes
- CVE-2022-34469: TLS certificate errors on HSTS-protected domains could be bypassed by the user on Firefox for Android
- CVE-2022-34471: Compromised server could trick a browser into an addon downgrade
- CVE-2022-34472: Unavailable PAC file resulted in OCSP requests being blocked
- CVE-2022-34478: Microsoft protocols can be attacked if a user accepts a prompt
- CVE-2022-2200: Undesired attributes could be set as part of prototype pollution
- CVE-2022-2226: An email with a mismatching OpenPGP signature date was accepted as valid
- CVE-2022-31746: Privileged internal URL protection could be bypassed through referrer header.

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. (**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 7.4: Perform Automated Application Patch Management:** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
- **Safeguard 7.7: Remediate Detected Vulnerabilities**
- **Safeguard 9.1: Ensure Use of Only Fully Supported Browsers and Email Clients**

- 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.

- 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™.

- Restrict use of certain websites, block downloads/attachments, block Javascript, restrict browser extensions, etc. (**M1021: Restrict Web-Based Content**)
    - **Safeguard 9.2: Use DNS Filtering Services:** Use DNS filtering services on all enterprise assets to block access to known malicious domains.
    - **Safeguard 9.3: Maintain and Enforce Network-Based URL Filters**
    - **Safeguard 9.6: Block Unnecessary File Types**

- 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.
- Block execution of code on a system through application control, and/or script blocking. (**M1038** : **Execution Prevention**)
    - **Safeguard 2.5 : Allowlist Authorized Software:** Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.
    - **Safeguard 2.6 : Allowlist Authorized Libraries:** Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, 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. Reassess bi-annually, or more frequently.
- Use capabilities to prevent suspicious behavior patterns from occurring on endpoint systems. This could include suspicious process, file, API call, etc. behavior. (**M1040 : Behavior Prevention on Endpoint**)
    - **Safeguard 13.2 : Deploy a Host-Based Intrusion Detection Solution**: Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.
    - **Safeguard 13.7 : Deploy a Host-Based Intrusion Prevention Solution:** Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.
- Blocking DNS traffic from servers outside of a configured allow-list. **(M1037: Filter Network Traffic)**
    - **Safeguard 4.9: Configure Trusted DNS Servers on Enterprise Assets:** Configure trusted DNS servers on enterprise assets. Example implementations include: configuring assets to use enterprise-controlled DNS servers and/or reputable externally accessible DNS servers.

Safeguard 13.4 : Perform Traffic Filtering Between Network Segments: Perform traffic filtering between network segments, where appropriate.

REFERENCES:

Mozilla:https://www.mozilla.org/en-US/security/advisories/mfsa2022-24/

https://www.mozilla.org/en-US/security/advisories/mfsa2022-25/

https://www.mozilla.org/en-US/security/advisories/mfsa2022-26/

https://www.mozilla.org/en-US/security/advisories/mfsa2022-27/

CISA:https://www.cisa.gov/uscert/ncas/current-activity/2022/06/29/mozilla-releases-security-updates-firefox-firefox-esr-and

CVE:https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2200

https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2226

https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31746

https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34468

https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34469

https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34470

https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34471

https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34472

https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34474

https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34476

https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34478

https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34481

https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34482

https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34483

https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34484