MS-ISAC® Cybersecurity Advisory

TLP:CLEAR
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER:
2023-029

DATE(S) ISSUED:
3/14/2023

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 111
- Firefox ESR versions prior to 102.9

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. CVE-2023-28176 and CVE-2023-28177 showed evidence of memory corruption and Mozilla presumes that with enough effort they could be exploited to run arbitrary code.

Details of these vulnerabilities are as follows:

Tactic: *Initial Access* (TA0001):

Technique: *Drive-by Compromise* (T1189)

- CVE-2023-28176: Memory safety bugs fixed in Firefox 111 and Firefox ESR 102.9
- CVE-2023-28177: Memory safety bugs fixed in Firefox 111

Additional lower priority vulnerabilities include:

- CVE-2023-28163: Windows Save As dialog resolved environment variables
- CVE-2023-25752: Potential out-of-bounds when accessing throttled streams

- CVE-2023-28162: Invalid downcast in Worklets
- CVE-2023-28164: URL being dragged from a removed cross-origin iframe into the same tab triggered navigation
- CVE-2023-25751: Incorrect code generation during JIT compilation
- CVE-2023-28159: Fullscreen Notification could have been hidden by download popups on Android
- CVE-2023-25748: Fullscreen Notification could have been hidden by window prompts on Android
- CVE-2023-25749: Firefox for Android may have opened third-party apps without a prompt
- CVE-2023-25750: Potential ServiceWorker cache leak during private browsing mode
- CVE-2023-28160: Redirect to Web Extension files may have leaked local path
- CVE-2023-28161: One-time permissions granted to a local file were extended to other local files loaded in the same tab

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:** Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.

  - **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.
- 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:** 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.
- 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.

REFERENCES:
Mozilla:
https://www.mozilla.org/en-US/security/advisories/mfsa2023-09/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-10/

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25748
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25749
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25750
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25751
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25752
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-28159
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-28160
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-28161
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-28162
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-28163
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-28164
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-28176
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-28177

Multi-State Information Sharing and Analysis Center (MS-ISAC)
Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061

24×7 Security Operations Center
SOC@cisecurity.org - 1-866-787-4722

TLP:CLEAR

www.cisa.gov/tlp

Information may be distributed without restriction, subject to standard copyright rules.