TLP: WHITE
https://www.cisa.gov/tlp

DATE(S) ISSUED:
09/08/2021

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

OVERVIEW:
Multiple vulnerabilities have been discovered in Mozilla Firefox, Firefox Extended Support Release (ESR), and 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. Successful exploitation 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 92
- Firefox ESR versions prior to 78.14
- Firefox ESR versions prior to 91.1
- Thunderbird versions prior to 78.14
- Thunderbird versions prior to 91.1

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **Medium**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in Mozilla Firefox, Firefox Extended Support Release (ESR), and Thunderbird, the most severe of which could allow for arbitrary code execution. Details of these vulnerabilities are as follows:

Mozilla Firefox
- Firefox for Android allowed navigations through the intent:// protocol, which could be used to cause crashes and UI spoofs. (CVE-2021-29993) *(This only affects Firefox for Android)*
- Mixed-content checks were unable to analyze opaque origins which led to some mixed content being loaded. (CVE-2021-38491)
- When delegating navigations to the operating system, Firefox would accept the mk scheme which might allow attackers to launch pages and execute scripts in Internet Explorer in unprivileged mode. (CVE-2021-38492) *(This only affects Firefox for Windows)*
- Improper Restriction of Operations within the Bounds of a Memory Buffer (CVE-2021-38493, CVE-2021-38494)

Firefox ESR 78.14
- When delegating navigations to the operating system, Firefox would accept the mk scheme which might allow attackers to launch pages and execute scripts in Internet Explorer in unprivileged mode. (CVE-2021-38492) (This only affects Firefox for Windows)
- Improper Restriction of Operations within the Bounds of a Memory Buffer (CVE-2021-38493)

Firefox ESR 91.1
- When delegating navigations to the operating system, Firefox would accept the mk scheme which might allow attackers to launch pages and execute scripts in Internet Explorer in unprivileged mode. (CVE-2021-38492) (This only affects Firefox for Windows)
- Improper Restriction of Operations within the Bounds of a Memory Buffer (CVE-2021-38495)

Firefox Thunderbird 78.14
- When delegating navigations to the operating system, Firefox would accept the mk scheme which might allow attackers to launch pages and execute scripts in Internet Explorer in unprivileged mode. (CVE-2021-38492) (This only affects Firefox for Windows)
- Improper Restriction of Operations within the Bounds of a Memory Buffer (CVE-2021-38493)

Firefox Thunderbird 91.1
- When delegating navigations to the operating system, Firefox would accept the mk scheme which might allow attackers to launch pages and execute scripts in Internet Explorer in unprivileged mode. (CVE-2021-38492) (This only affects Firefox for Windows)
- Improper Restriction of Operations within the Bounds of a Memory Buffer (CVE-2021-38495)

Successful exploitation 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/mfsa2021-38/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-39/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-40/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-41/
https://www.mozilla.org/en-US/security/advisories/mfsa2021-42/

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29993
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38491
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38492
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38493
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38494
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38495

TLP: WHITE
https://www.cisa.gov/tlp