*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**
**Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.**
**http://www.us-cert.gov/tlp/**

**DATE(S) ISSUED:**
01/07/2021
***01/12/2021 - UPDATED***

**SUBJECT:**
A Vulnerability in Mozilla Firefox Could Allow for Arbitrary Code Execution

**OVERVIEW:**
A vulnerability has been discovered in Mozilla Firefox, Firefox Extended Support Release (ESR) and Firefox for Android, 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. Firefox for Android is a version of the web browser used on Android based mobile devices. Successful exploitation of this vulnerability 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.

***January 12 – UPDATED OVERVIEW:***

***A vulnerability has been discovered in Mozilla Firefox, Firefox Extended Support Release (ESR) Firefox for Android, and Mozilla Thunderbird 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.***
- ***Firefox for Android is a version of the web browser used on Android based mobile devices.***
- ***Mozilla Thunderbird is an open-source email, chat, and RSS client.***

***Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights post-exploitation. Users whose accounts are configured to have fewer user rights on the system could be less impacted and pose less of a risk than those operating with administrative user rights.***

**THREAT INTELLIGENCE:**
There are currently no reports of this vulnerability being exploited in the wild.

**SYSTEMS AFFECTED:**

- Mozilla Firefox versions prior to 84.0.2
- Mozilla Firefox ESR versions prior to 78.6.1
- Firefox for Android versions prior to 84.1.3

***January 12 – UPDATED SYSTEMS AFFECTED:***

- ***Mozilla Thunderbird versions prior to 78.6.1***

**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:**
A vulnerability has been discovered in Mozilla Firefox, Mozilla Firefox Extended Support Release (ESR), and Firefox for Android, 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. Firefox for Android is a version of the web browser used on Android based mobile devices. Details of the vulnerability are as follows:

- In certain circumstances, the COOKIE-ECHO chunk in an SCTP packet can be modified in a way that results in an exploitable use-after-free condition. (CVE-2020-16044)

Successful exploitation of this vulnerability 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/mfsa2021-01/#CVE-2020-16044

**CVE:**
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16044

***January 12 – UPDATED REFERENCES:***
***Mozilla:***
***https://www.mozilla.org/en-US/security/advisories/mfsa2021-02/***