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.
https://www.us-cert.gov/tlp/

DATE(S) ISSUED:
06/14/2019

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

OVERVIEW:
Multiple vulnerabilities have been identified in Mozilla Thunderbird, the most severe of which could allow for arbitrary code execution. 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 Thunderbird versions prior to 60.7.1

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:
Multiple vulnerabilities have been identified in Mozilla Thunderbird, the most severe of which could allow for arbitrary code execution. In general, these flaws cannot be exploited through email in the Thunderbird product because scripting is disabled when reading mail, but are potentially risks in browser or browser-like contexts. Details of the vulnerabilities are as follows:

- A flaw in Thunderbird's implementation of iCal causes a heap buffer overflow in parser_get_next_char when processing certain email messages, resulting in a potentially exploitable crash. (CVE-2019-11703)

- A flaw in Thunderbird's implementation of iCal causes a heap buffer overflow in icalmemory_strdup_and_dequote when processing certain email messages, resulting in a potentially exploitable crash. (CVE-2019-11704)
- A flaw in Thunderbird's implementation of iCal causes a stack buffer overflow in icalrecur_add_bydayrules when processing certain email messages, resulting in a potentially exploitable crash. (CVE-2019-11705)
- A flaw in Thunderbird's implementation of iCal causes a type confusion in icaltimezone_get_vtimezone_properties when processing certain email messages, resulting in a crash. (CVE-2019-11706)

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

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/mfsa2019-17/

CVE:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11703
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11704
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11705
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11706

message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

Chris Watts
Security Operations Analyst
MS Department of Information Technology Services
601-432-8201 | www.its.ms.gov