TLP: WHITE
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER: 2018-110

DATE(S) ISSUED: 10/05/2018

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 result in 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 60.2.1

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 result in arbitrary code execution. Details of these vulnerabilities are as follows:

- A use-after-free vulnerability can occur when refresh driver timers are refreshed in some circumstances during shutdown when the timer is deleted while still in use. This results in a potentially exploitable crash. (CVE-2018-12377)
- A use-after-free vulnerability can occur when an IndexedDB index is deleted while still in use by JavaScript code that is providing payload values to be stored. This results in a potentially exploitable crash. (CVE-2018-12378)
- When the Mozilla Updater opens a MAR format file which contains a very long item filename, an out-of-bounds write can be triggered, leading to a potentially exploitable crash. This requires running the Mozilla Updater manually on the local system with the malicious MAR file in order to occur. (CVE-2018-12379)
- Browser proxy settings can be bypassed by using the automount feature with autofs to create a mount point on the local file system. Content can be loaded from this mounted file system directly using a file: URI, bypassing configured proxy settings. Note: this issue only affects OS X in default configurations. On Linux systems, autofs must be installed for the vulnerability to occur and Windows is not affected. (CVE-2017-16541)

- Memory safety bugs present in Firefox 61 and Firefox ESR 60.1. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. (CVE-2018-12376)
- A potentially exploitable crash in TransportSecurityInfo used for SSL can be triggered by data stored in the local cache in the user profile directory. This issue is only exploitable in combination with another vulnerability allowing an attacker to write data into the local cache or from locally installed malware. This issue also triggers a non-exploitable startup crash for users switching between the Nightly and Release versions of Firefox if the same profile is used. (CVE-2018-12385)
- If a user saved passwords before Firefox 58 and then later set a master password, an unencrypted copy of these passwords is still accessible. This is because the older stored password file was not deleted when the data was copied to a new format starting in Firefox 58. The new master password is added only on the new file. This could allow the exposure of stored password data outside of user expectations. (CVE-2018-12383)

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.
- 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/mfsa2018-25/

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12376
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12377
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12378
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12379
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12383
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12385
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-16541

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

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/