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
https://www.cisa.gov/tlp
Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

DATE(S) ISSUED:
12/02/2021

SUBJECT:
A Vulnerability in Mozilla NSS (Network Security Services) Could Allow for Arbitrary Code Execution

OVERVIEW:
A vulnerability has been discovered in Mozilla's Network Security Services (NSS), a set of cryptography libraries used to handle signatures and certification validation. Successful exploitation of this vulnerability could allow for arbitrary code execution within the context of the affected application, which could be either a client like Thunderbird or server like Apache webserver. Depending on the privileges associated with this application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of this vulnerability could have less impact than if it was configured with administrative rights.

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

SYSTEMS AFFECTED:
- NSS (Network Security Services) versions prior to 3.73 or 3.68.1 ESR

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's Network Security Services (NSS), a set of cryptography libraries used to handle signatures and certification validation. Successful exploitation of this vulnerability could allow for arbitrary code execution within the context of the affected application, which could be either a client like Thunderbird (connection with attacker TLS server) or server like Apache webserver (processing client certificate).

Per Mozilla:

> "Applications using NSS for handling signatures encoded within CMS, S/MIME, PKCS #7, or PKCS #12 are likely to be impacted. Applications using NSS for certificate validation or other TLS, X.509, OCSP or CRL functionality may be impacted, depending on how they configure NSS."

NSS is used in software such as:

- Thunderbird
- mod_nss SSL module for the Apache webserver
- Red Hat Directory Server
- Oracle Directory Server Enterprise Edition

Per Red Hat:

> "Firefox is not vulnerable to this flaw as it uses the mozilla::pkix for certificate verification. Thunderbird is affected when parsing email with the S/MIME signature. Thunderbird on Red Hat Enterprise Linux 8.4 and later does not need to be updated since it uses the system NSS library, but earlier Red Hat Enterprise Linux 8 extended life streams will need to update Thunderbird as well as NSS."

Successful exploitation of this vulnerability could allow for arbitrary code execution within the context of the affected application, which could be either a client like Thunderbird or server like Apache webserver. Depending on the privileges associated with this application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of this vulnerability could have less impact than if it was configured with administrative rights.

RECOMMENDATIONS:

The following actions should be taken:

- If applications used within the organization are known to use SSL/TLS, verify if Mozilla NSS is being used.
- Apply the latest patches provided by respective vendors after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43527

Mozilla:
https://www.mozilla.org/en-US/security/advisories/mfsa2021-51/

Google Project Zero:
https://googleprojectzero.blogspot.com/2021/12/this-shouldnt-have-happened.html

Bleeping Computer:
https://www.bleepingcomputer.com/news/security/mozilla-fixes-critical-bug-in-cross-platform-cryptography-library/

Red Hat:
https://access.redhat.com/security/cve/CVE-2021-43527

TLP: WHITE
https://www.cisa.gov/tlp
Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.