**Mozilla NSS**

Mozilla NSS (Network Security Services) is a set of libraries that provide cryptographic and security functionality for applications. The NSS library provides several cryptographic features such as SSL/TLS, Cryptographic algorithms, Certificate management and Key management, thereby, making it powerful and flexible for developers to implement strong cryptographic security. NSS can be used on various operating systems such as Windows, Linux, and macOS and is licensed under Additionally, NSS is licensed under the permissive open-source license i.e., Mozilla Public License.

**CVE-2021-43527**

It is a software-based vulnerability that affects server as well as client applications using NSS versions before 3.73 ESR. The way NSS verifies certificates has been determined to have a remote code execution issue. When a client application built using NSS tries to establish an SSL/TLS connection, this weakness enables an attacker acting as an SSL/TLS server to cause this problem. The weakness can also be exploited by a server application built using NSS that processes client certificates and receives a rogue certificate from a client. Confidentiality, integrity, and system availability pose the most risk to this vulnerability.

When handling DSA or RSA-PSS signatures that have been DER-encoded, NSS (Network Security Services) versions are susceptible to a heap overflow. Applications that use NSS for signatures encoded in CMS, S/MIME, PKCS \#7, or PKCS \#12 are likely to be impacted. Additionally, applications using NSS for certificate validation or other TLS, X.509, OCSP or CRL functionality are affected. This basically depends on how NSS is installed.

Red Hat, Thunderbird, LibreOffice, Evolution, and Evince are among the programmes that are vulnerable since they use NSS for signature verification, in contrast to Mozilla's Firefox web browser, email client, and PDF viewers, which are secure from the vulnerability.

The vulnerability is due to a bug in the certificate verification code in the vfy\_CreateContext function of the secvfy.c file. The error manifests itself both when the client reads the certificate from the server as well as when the server processes the client's certificates.

In order to prevent this vulnerability, first, we should verify if Mozilla NSS is being used in organisations applications using SSL/TLS. Then, latest security patches should be applied after proper testing. in order to mitigate the attack, all the software should be run as a a common user. Last, least privilege should be granted to all the accounts.

**Protocol Based Vulnerability**

The SSLv2 protocol's design includes a flaw since client master keys, whose authenticity is decided by the first step of the SSL handshake, are used to produce session keys. Buffer overflow is brought on by the client master key's incorrect length. An exploitable buffer overflow exists.

Using the privileges of the user executing the application, the attacker can run the code. Moreover, a hacker might launch a denial-of-service attack.

By turning off SSLv2 support, this vulnerability can be protected against. Firefox 2.0.0.2, Firefox 1.5.0.10, SeaMonkey 1.0.8, and NSS 3.11.5 all get around this.

References

1. <https://www-archive.mozilla.org/projects/security/pki/nss/>
2. <https://firefox-source-docs.mozilla.org/security/nss/index.html>
3. <https://cyberdaily.securelayer7.net/vulnerability-in-mozilla-nss-crypto-library-impacts-software>
4. <https://access.redhat.com/security/cve/cve-2021-43527>
5. <https://access.redhat.com/security/vulnerabilities/RHSB-2021-008>
6. <https://googleprojectzero.blogspot.com/2021/12/this-shouldnt-have-happened.html>
7. <https://www.linuxadictos.com/en/bigsig-una-vulnerabilidad-en-mozilla-nss-que-podria-permitir-la-ejecucion-de-codigo.html>
8. https://www.kb.cert.org/vuls/id/592796