**MatrixSSL**

MatrixSSL is the first open-source small footprint SSL stack and is also known as Inside Secure TLS Toolkit. It is offered in the form of a Software Development Kit (SDK) that is geared towards application in Internet of Things (IOT) devices and other embedded systems. An open-source TLS/SSL implementation is made for use in embedded hardware settings. For Internet of Things (IoT) devices with small footprints and minimal connection overhead, MatrixSSL is an embedded SSL and TLS implementation with minimum dependencies on portability.

MatrixSSL uses public key algorithms such RSA, Diffie-Hellman Algorithm, etc. and symmetric algorithms such as AES, ChaCha20-Poly1305 and other algorithms as well as client and server support for TLS 1.3, mutual authentication, session resumption, and other features. There are portability levels for additional OS systems, cypher suites, and cryptography providers in the well-documented source, which also includes these features.

**Vulnerabilities**

Among multiple vulnerabilities associated with MatrixSSL, some of the more popularly known vulnerabilities are mentioned below:

1. **CVE-2022-43974:** CVE-2022-43974 is a buffer overflow vulnerability found in MatrixSSL versions 4.5.1-4.0.0 that could allow information disclosure and remote code execution. An attacker could use a network link to overwrite the data in RAM on a server running MatrixSSL if there was a buffer overflow (TLS Toolkit). This vulnerability has been demonstrated to be usable for a denial-of-service attack. Additionally, it might be possible for an attacker to exploit this vulnerability to install and execute malicious code.

It is feasible to trick the TLS1.3 'change cypher spec' processing to result in an integer overflow by using a specifically crafted packet. All MatrixSSL (TLS Toolkit) versions that enable TLS1.3 have the matrixSslDecodeTls13() function implemented incorrectly. It was found and reported by security analysts Robert Hörr and Alissar Ibrahim from Deutsche Telekom's IT Security Evaluation Facility, and was fixed in version 4.6.0, which was made available in December 2022.

1. **CVE-2019-14431:** The DTLS server faces issues while handling inbound network messages in MatrixSSL versions 3.8.3 Open through 4.2.1 Open and hence causing a heap-based buffer overflow of up to 256 bytes and Remote Code Execution. During this process of mishandling of the crafted data packets, the server handles the fragment length value provided with the DTLS messages in an incorrect manner.

Table

Description automatically generated

Text

Description automatically generated with low confidence

1. **CVE-2018-12439:** This vulnerability uses the Return of The Hidden Number Problem, also known as ROHNP to challenge ECDSA signatures using MatrixSSL through version 3.9.5 Open. The attacker requires access to either the local computer or another virtual machine running on the same physical host in order to find out an ECDSA key. The vulnerability exposes sensitive information to an attacker or the outside world that is not explicitly authorized to have access to that information.
2. **CVE-2017-1000415**: The SSL/TLS protocol has long utilised the X.509 Public-Key Infrastructure to accomplish authentication. Its popularity in the recent times has been further boosted by a new trend called Internet-of-Things (IoT) devices using small footprint SSL/TLS libraries for secure communication. The X.509 security assurances rely on the underlying implementation's strict examination of X.509 certificate chains and acceptance of only legitimate ones. Implementations of X.509 that are not compliant run the risk of causing attacks and/or compatibility problems.

This vulnerability is related to the X.509 certificate validation process in MatrixSSL. The X.509 certificate validation procedure in MatrixSSL version 3.7.2 incorrectly validates UTCTime date ranges, which causes some certificates to have their expiration (beginning) year extended (delayed) by 100 years.

Diagram

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Timeline

Description automatically generated with medium confidence

**References**

<https://www.nccgroup.trust/us/our-research/technical-advisory-return-of-the-hidden-number-problem/>

<https://www.helpnetsecurity.com/2023/01/13/fuzzing-cryptographic-libraries/#:~:text=CVE%2D2022%2D43974%20is%20a,disclosure%20and%20remote%20code%20execution>.

<https://nvd.nist.gov/vuln/detail/CVE-2022-43974>

<https://github.com/matrixssl/matrixssl/security/advisories/GHSA-fmwc-gwc5-2g29>

<https://cve.report/CVE-2018-12439>

<https://nvd.nist.gov/vuln/detail/CVE-2019-14431>

<https://www.ieee-security.org/TC/SP2017/papers/231.pdf>