MQTTSA Report

Authentication

[!] MQTTSA did not detect an authentication mechanism
The tool was able to connect to the broker without specifying any kind of credential information. This may cause remote attackers to successfully connect to the broker.

Suggested mitigations

It is strongly recommended to implement an authentication mechanism, so that only devices which are authenticated can interact with the broker. We suggest to implement authentication through X.509 certificates, however, a username/password enforcement can work as well, if a strong password is used.
Additional information here:

MQTT Security Fundamentals: Authentication with Username and Password
Wikipedia: Password Strenght
MQTT Security Fundamentals: X509 Client Certificate Authentication
ThingsBoard: X.509 Certificate Based Authentication

Information disclosure

MQTTSA waited for 60 seconds after having subscribed to the '#' and '$SYS/#' topics. By default, clients who subscribe to the '#' topic can read to all the messages exchanged between devices and the ones subscribed to '$SYS/#' can read all the messages which includes statistics of the broker. Remote attackers could obtain specific information about the version of the broker to carry on more specific attacks or read messages exchanged by clients.

[!] MQTTSA successfully intercepted all the messages belonging to 4 topics, 2 of them non $SYS.
The non-SYS topics are: ['topic1', 'topic2']
The SYS topics are: ['sys1', 'sys2']

Suggested mitigations

It is strongly recommended to enforce an authorization mechanism in order to grant the access to confidential resources only to the specified users or devices. There are two possible approaches: Access Control List (ACL) and Role-based Access Control (RBAC). Unfortunately, the current version of MQTT support authorization only broker-side.
Additional information here:

Wikipedia: Access Control List
Wikipedia: Role-based Access Control
MQTT Security Fundamentals: Authorization
Configuring and Testing Mosquitto MQTT Topic Restrictions

Information disclosure

MQTTSA waited for 60 seconds after having subscribed to the '#' and '$SYS/#' topics. By default, clients who subscribe to the '#' topic can read to all the messages exchanged between devices and the ones subscribed to '$SYS/#' can read all the messages which includes statistics of the broker. Remote attackers could obtain specific information about the version of the broker to carry on more specific attacks or read messages exchanged by clients.

[!] In this case, MQTTSA was unable to intercept messages exchanged by clients. Try to perform the assessment again, increasing the 'listening_time' parameter

Tampering data

After having successfully intercepted some messages, MQTTSA automatically created a new message (having as a payload the string 'ciao') and send it into every topic it is able to intercept. Remote attackers could exploit it to write in specific topics pretending to be a specific device and send tampered measures.

[!] MQTTSA was able to write in 2 topics, with 1 of them being non-$SYS.
The topics were: ['aa'] ['a']

Suggested mitigations

The implementation of an authorization mechanism can mitigate this risk. Check the "Mitigations" paragraph in the section "Information disclosure".