MQTTSA Report

[!] No authentication mechanism detected

MQTTSA detect that no authentication mechanism is put in place in the specified broker. 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 and read and write MQTT messages exchanged between clients.

Suggested mitigations

Implement an authentication mechanism, so that only devices which are authenticated can successfully connect to the broker.
Additional information here:
MQTT Security Fundamentals: Authentication with Username and Password

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 topics non SYS are:
topic1
topic2

The topics SYS are:
sys1
sys2

Suggested mitigations

Implement the MQTT protocol to work over TLS, as reported in the official documentation of MQTT. TLS provides a secure communication channel between client and server, thus, assuming the use of a secure version of TLS and cipher suites, the content of the communication cannot be read by attackers.
ATTENTION! Using MQTT over TLS could lead to a communication overhead and an increase of CPU usage, especially during the handshake. In devices which have constrained resources, TLS could have a severe impact. In these cases there are other solutions that could be used to secure the communication, such as encrypting only specific messages (for instance CONNECT and PUBLISH). Instead, in case the MQTT implementation can afford it, it is advisable to use further security mechanisms, such as payload encryption and signature verifications. An additional mitigation could be the implementation of an authorization mechanism (such as Access Control List), in order to prevent unauthorized users to listen to specific topics.
Additional information here:
MQTT security fundamentals: TLS / SSL
how does TLS affect MQTT performance?