MQTTSA Report

Details of the assessment

Broker ip: test.mosquitto.org
Listening time: 60
Text message: testtesttest
Denial of Service performed: False
Brute force performed: False

Authentication

MQTTSA detected an authentication mechanism.

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 not able to intercept messages exchanged by clients. Try to perform the assessment again, increasing the 'listening_time' parameter

Tampering data

[!] Since MQTTSA was not able to intercept any message, this vulnerability was not tested. Try to perform the assessment again, increasing the 'listening_time' parameter.

Denial of service

[!] MQTTSA opened None connections to stress the broker and test how it will react in case of Denial of Service.
The tool is not able to determine if the test resulted in the disconnection of other clients; thus the user should check the logfile in the broker and see if the connection was working correctly.
In case the test did not result in disconnections or delays, the test can be performed again increasing the *dos_connection* value.

Suggested mitigations

In case of MQTT services connected in environments with limited bandwidth capacity, it is strongly recommended to: add a firewall and enforce rules to prevent the Dos, use a load balancer, limit the number of clients and packet dimension.
Additional information here:
MQTT Security Fundamentals: Securing MQTT Systems
Mosquitto documentation: message_size_limit and max_connection

Malformed data

[!] MQTTSA tried to stress the broker by sending malformed packets in the Topic1 topic.

An attacker could send malformed packets aiming at triggering errors to cause DoS or obtain information about the broker. We suggest to perform a full fuzzing test to stress the implementation with random well-crafted values. A fuzzer designed for MQTT is developed by F-Secure and can be found on the following link:

[Fuzzer F-Secure]

Parameter of the CONNECT packet tested: client_id

Values that did not generate an error:

test, , testtesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttes
ttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttestte
sttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttestt
esttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttest
testtesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttest

Values that generated an error and the related error:

Parameter of the CONNECT packet tested: clean_session

Values that did not generate an error:

True, 1, 2

Values that generated an error and the related error:

Value: False, Error: A client id must be provided if clean session is False.

Value: 0, Error: A client id must be provided if clean session is False.

Value: -1, Error:

Parameter of the CONNECT packet tested: userdata

Values that did not generate an error:

test, , testtesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttes
ttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttestte
sttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttestt
esttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttest
testtesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttest

Values that generated an error and the related error:

Parameter of the CONNECT packet tested: keepalive

Values that did not generate an error:

0, 1, 2, 234, 0.12

Values that generated an error and the related error:

Value: 3, Error: [Errno 101] Network is unreachable

Value: -1, Error: Keepalive must be >=0.

Value: -100, Error: Keepalive must be >=0.

Value: -0.12, Error: Keepalive must be >=0.

Value: 893427908127340981723498712309487120937492813749721394719023740971230948710293847091273409871230

4971029374912837409723901740923740912374907120934709123749032 1, Error: integer out of range for 'H' format code

Value:
-1928349182037498127349871239047092387409723104971230947923749012730497210934871293074923174921379047012347092734, Error: Keepalive must be >=0.

Parameter of the PUBLISH packet tested: topic

Values that did not generate an error:
///////, /../../../../

Values that generated an error and the related error:
Value: #, Error: Publish topic cannot contain wildcards.
Value: /#/#/#, Error: Publish topic cannot contain wildcards.

Parameter of the PUBLISH packet tested: payload

Values that did not generate an error:
test, ,
test

Values that generated an error and the related error:

Parameter of the PUBLISH packet tested: qos

Values that did not generate an error:
0, 1, 2

Values that generated an error and the related error:
Value: 3, Error: Invalid QoS level.
Value: -1, Error: Invalid QoS level.
Value: -100, Error: Invalid QoS level.
Value: 234, Error: Invalid QoS level.
Value: 0.12, Error: unsupported operand type(s) for <<: 'float' and 'int'
Value: -0.12, Error: Invalid QoS level.
Value:
8934279081273409817234987123094871209374928137497213947190237409712309487102938470912734098712304971029374912837409723901740923740912374907120934709123749032 1, Error: Invalid QoS level.
Value:
-1928349182037498127349871239047092387409723104971230947923749012730497210934871293074923174921379047012347092734, Error: Invalid QoS level.