MQTTSA Report

Details of the assessment

Broker ip: mqtt.fluux.io
Listening time: 2
Text message: testtesttest
Denial of Service performed: True
Brute force performed: True

Authentication

MQTTSA detected an authentication mechanism.

Information disclosure

MQTTSA waited for 2 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 221 topics, 221 of them non $SYS.
The non-SYS topics are: ['/541988642/541988658/3891256539/49', '/541996658/541996674/4958866082/17',
'/541995842/541995858/3793806713/78', '/541992242/541992258/9115749946/34',
'/541994738/541994754/7295040319/72', '/541991522/541991538/7954794810/21',
'/541993058/541993074/3968064784/38', '/541995506/541995522/1201829564/68',
'/541989506/541989522/3466928416/67', '/541990274/541990290/5707255580/14',
'/541986914/541986930/5638246780/71', '/541996898/541996914/8326620339/67',
'/541993010/541993026/4966613994/85', '/541986962/541986978/941954467/81',
'/541989698/541989714/4019571539/57', '/541994498/541994514/5109498432/99',
'/541996130/541996146/3562716687/59', '/541989026/541989042/1022243404/61',
'/541987730/541987746/1195639664/21', '/541988930/541988946/86176817/76',
'/541988210/541988226/1084752878/71', '/541995554/541995570/7312493080/19',
'/541990658/541990674/812660808/92', '/541990946/541990962/3794211630/43',
'/541989410/541989426/3765475862/96', '/541987586/541987602/8976784419/67',
'/541994786/541994802/3234767678/24', '/541991090/541991106/6609409371/27',
'/541988114/541988130/595358904/91', '/541994834/541994850/8753990895/50',
'/541989458/541989474/4606396220/37', '/541991570/541991586/2394321598/60',
'/541995986/541996002/1831344989/35', '/541991426/541991442/2395330924/25',
'/541987682/541987698/1689454004/8', '/541995122/541995138/2036487736/98',
'/541994546/541994562/4326551845/39', '/541990178/541990194/4536924050/43',
'/541988450/541988466/7816039067/47', '/541992290/541992306/568432360/62',
'/541992914/541992930/214516474/82', '/541988162/541988178/8085771141/2',
'/541995698/541995714/709027598/14', '/541994882/541994898/2405282997/46',
'/541993730/541993746/8198042890/57', '/541990850/541990866/5217530951/95',
'/541987970/541987986/817050400/11', '/541989794/541989810/5777996686/11',
'/541988306/541988322/3216136448/37', '/541989554/541989570/3051677784/85',
'/541991330/541991346/7163770919/86', '/541995938/541995954/2268402158/49',
'/541987298/541987314/9244378544/28', '/541989986/541990002/7365080232/78',
'/541991186/541991202/5113026131/68', '/541993778/541993794/6604148644/80',
'/541986674/541986690/3720700656/44', '/541995410/541995426/7761852887/90',
'/541992674/541992690/6847438595/29', '/541986722/541986738/9200824745/9',
'/541996610/541996626/2221274080/32', '/541995458/541995474/406983305/73',
'/541993490/541993506/902383307/66', '/541991666/541991682/860788068/70', 'netq_unixweb/digiop/op',

'/541992866/541992882/7549815628/26', '/541996178/541996194/3626785765/88',
'/541988018/541988034/3279495176/92', '/541996418/541996434/362772782/15',
'/541992722/541992738/2969147259/81', '/541990994/541991010/3719408265/97',
'/541993154/541993170/4681914942/54', '/541992626/541992642/9573328970/5',
'/541987778/541987794/3440429421/36', '/541996226/541996242/267778405/57',
'/541995362/541995378/6403672980/35', '/541988834/541988850/2336083185/48',
'/541987922/541987938/7427366508/98', '/541986482/541986498/2975004151/97',
'/541990130/541990146/1634340465/11', '/541996082/541996098/7210328433/95',
'/541994066/541994082/1292788512/7', '/541993106/541993122/5499268626/51',
'/541991810/541991826/5362563135/36', '/541994594/541994610/2894293635/21',
'/541994450/541994466/9630285830/14', '/541995602/541995618/515869605/39',
'/541987634/541987650/2411565371/58', '/541987394/541987410/1783144882/19',
'/541994018/541994034/9042997274/63', '/541988066/541988082/3293717095/13',
'/541994162/541994178/41007591/38', '/541996274/541996290/5228128726/78',
'/541992002/541992018/250199171/40', '/541990754/541990770/1870907994/46',
'/541991618/541991634/2810347712/91', '/541988546/541988562/6287017021/93',
'/541992578/541992594/7988773705/75', '/541989602/541989618/1437319549/47',
'/541996706/541996722/4730107844/58', 'netq_unixweb/digiin/in', '/541991138/541991154/7565300616/55',
'/541990226/541990242/2737823672/79', '/541989074/541989090/7586608158/60',
'/541990034/541990050/1729236761/78', '/541990898/541990914/5246093931/70',
'/541991378/541991394/6972685713/41', '/541995266/541995282/6803533615/92',
'/541994402/541994418/1849936887/28', '/541995218/541995234/5648649936/20',
'/541986818/541986834/4882715425/23', '/541994978/541994994/1584660757/31',
'/541995314/541995330/6453432223/75', '/541987874/541987890/2087605839/58',
'/541987826/541987842/800799021/88', '/541994930/541994946/2229454756/29',
'/541990370/541990386/5625921946/97', '/541991042/541991058/1211956180/19',
'/541993826/541993842/1811305346/43', '/541996034/541996050/6764416501/66',
'/541988402/541988418/3131306072/34', '/541994306/541994322/7490667313/21',
'/541994642/541994658/694992109/18', '/541993586/541993602/3039271096/40',
'/541995794/541995810/4339512032/32', '/541992050/541992066/7148942728/100',
'/541987442/541987458/9206959552/67', '/541989122/541989138/6175866307/76',
'/541989650/541989666/7956464805/40', '/541993346/541993362/908935742/81',
'/541996322/541996338/7276682449/74', '/541987058/541987074/6453649027/27',
'/541988498/541988514/9444946308/34', '/541986626/541986642/5828048500/22',
'/541995026/541995042/3543590864/99', '/541996562/541996578/8464917481/58',
'/541991858/541991874/3055262703/66', '/541990514/541990530/9571138135/81',
'/541990706/541990722/8205911070/78', '/541988354/541988370/7208956091/64',
'/541993634/541993650/6251204109/82', '/541992482/541992498/7839348267/44',
'/541996370/541996386/2089756877/20', '/541989842/541989858/7541875476/38',
'/541989170/541989186/9501993933/33', '/541988690/541988706/9951396255/10',
'/541996514/541996530/5849933888/32', '/541992530/541992546/4609167049/30',
'/541994354/541994370/5752054636/18', '/541993298/541993314/63922399/4',
'/541987538/541987554/4788196093/14', '/541990802/541990818/268113029/58',
'/541995650/541995666/1413741072/25', '/541987202/541987218/9755896910/69',
'/541991906/541991922/5958482870/85', '/541990082/541990098/5896174938/94',
'/541991234/541991250/7079938782/71', '/541993970/541993986/6425001495/92',
'/541996754/541996770/4837983428/63', '/541993874/541993890/2597876143/9',
'/541993394/541993410/9011788727/92', '/541988786/541988802/2354849263/27',
'/541990466/541990482/273110101/57', '/541994114/541994130/7068655297/44',
'/541993202/541993218/4184267638/14', '/541989218/541989234/6816149927/43',
'/541986770/541986786/8733371794/16', '/541992434/541992450/926951090/33',
'/541995170/541995186/5144744528/55', '/541991762/541991778/8426184429/74',
'/541987346/541987362/2583510332/45', '/541991282/541991298/668810192/24',
'/541992770/541992786/1227509887/3', '/541992962/541992978/4630342154/75',
'/541988258/541988274/9271190604/27', '/541995890/541995906/694853248/96',
'/541993250/541993266/3947560650/23', '/541994258/541994274/2417356491/57',
'/541995746/541995762/5686303816/76', '/541989362/541989378/9620683093/74',
'/541992146/541992162/6513930837/29', '/541993538/541993554/2923495341/36',
'/541989746/541989762/5279520273/43', '/541988978/541988994/9008416143/79',
'/541994210/541994226/5949702596/63', '/541986530/541986546/8113666581/33',
'/541989890/541989906/2057233422/43', '/541991714/541991730/7222744608/44',
'/541990610/541990626/407109723/1', '/541996946/541996962/878388921/50',
'/541989938/541989954/7484373799/36', '/541986578/541986594/2363819589/54',

'/541993682/541993698/2166776049/27', '/541987106/541987122/9523096798/35',
'/541989314/541989330/6792570861/83', '/541996802/541996818/2311957668/24',
'/541988738/541988754/6903331539/77', '/541992386/541992402/303216331/9',
'/541987010/541987026/4722264883/18', '/541988882/541988898/2599951166/56',
'/541986866/541986882/1811550027/61', '/541996850/541996866/1848117653/67',
'/541987490/541987506/7793736819/76', '/541992098/541992114/6330578158/52',
'/541992818/541992834/3725421848/34', '/541987154/541987170/968330795/64',
'/541991954/541991970/542629693/54', '/541987250/541987266/9741633504/77',
'/541992338/541992354/8242443493/57', '/541990322/541990338/9853976333/68',
'/541990562/541990578/6496483063/48', '/541991474/541991490/983325536/77',
'/541989266/541989282/1958526155/28', '/541995074/541995090/755191603/43',
'/541996466/541996482/4349381121/44', '/541988594/541988610/2460690707/23',
'/541993442/541993458/9691061886/27', '/541992194/541992210/1928325933/44',
'/541994690/541994706/9577424552/29', '/541993922/541993938/3944468109/28',
'/541990418/541990434/2554744859/4']

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
MQTT Security Fundamentals: OAuth 2.0 & MQTT
Configuring and Testing Mosquitto MQTT Topic Restrictions

Tampering data

After having successfully intercepted some messages, MQTTSA automatically created a new message (having as a payload the string 'testtesttest') 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 20 topics, with 20 of them being non-$SYS.
The topics were: ['netq_unixweb/digiin/in', '/541986914/541986930/5638246780/71',
'/541987250/541987266/9741633504/77', '/541986962/541986978/941954467/81',
'/541987202/541987218/9755896910/69', '/541986722/541986738/9200824745/9',
'/541986626/541986642/5828048500/22', '/541987010/541987026/4722264883/18',
'/541987058/541987074/6453649027/27', '/541986818/541986834/4882715425/23',
'/541986530/541986546/8113666581/33', 'netq_unixweb/digiop/op', '/541986866/541986882/1811550027/61',
'/541986482/541986498/2975004151/97', '/541986770/541986786/8733371794/16',
'/541986578/541986594/2363819589/54', '/541986674/541986690/3720700656/44',
'/541987154/541987170/968330795/64', '/541987106/541987122/9523096798/35',
'/541987298/541987314/9244378544/28'] []

Suggested mitigations

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

Brute force

The brute force test can not be performed. Authentication mechanism may not use username/password or not be

enforced at all, check the Authentication section.

Denial of service

[!] MQTTSA opened 2 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 netq_unixweb/digiin/in 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, ,
testtesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttes
ttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttestte
sttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttestt
esttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttest
testtesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttest

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, -1

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.

Parameter of the CONNECT packet tested: userdata

Values that did not generate an error:

test, ,
testtesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttes
ttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttestte
sttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttestt
esttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttest
testtesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttest

Values that generated an error and the related error:

Parameter of the CONNECT packet tested: keepalive

Values that did not generate an error:

1, 2, 3, 234, 0.12

Values that generated an error and the related error:

Value: 0, Error: The operation did not complete (read) (_ssl.c:590)

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

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

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

Value:
8934279081273409817234987123094871209374928137497213947190237409712309487102938470912734098712304971029374912837409723901740923740912374907120934709123749032 1, Error: integer out of range for 'H' format code

Value:
-192834918203749812734987123904709238740972310497123094792374901273049721093487129307492317492137 9047012347092734, 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, ,
testtesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttes
ttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttestte
sttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttestt
esttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttest
testtesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttesttest

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: 893427908127340981723498712309487120937492813749721394719023740971230948710293847091273409871230497102937491283740972390174092374091237490712093470912374903 21, Error: Invalid QoS level.
Value: -192834918203749812734987123904709238740972310497123094792374901273049721093487129307492317492137904701234709 2734, Error: Invalid QoS level.