rmqtt

H3 攻击场景与漏洞危害

考虑共享场景下的物联网应用，即智能家居系统使用MQTT协议进行物联网设备和用户管理，其中有两个用户角色。管理员（即房主）可以授权其他普通用户（例如，客人、租户）访问他的智能家居设备的权利。普通用户的访问权限可能会被撤销（租约到期）。我们认为管理员和设备是良性的，而客人可能是恶意的，会尽可能地去试图越权访问设备（越权或是维持被撤销的权限）。

H5 0x01攻击场景

首先，攻击者拥有连接broker的权限（需要在broker上有一个账号和密码）

01. 受害者（clean start=false，表示在服务器上保留会话）连接到broker
02. 受害者订阅了相关主题（如“testtopic”）
03. 攻击者使用与受害者相同的clientID连接（clean start=false）到broker

04. 智能设备向受害者订阅的话题（“testtopic”）发布消息，消息将被转发给攻击者（即使攻击者不具有订阅权限）

H5 0x02漏洞危害

攻击者能够在没有订阅权限的情况下收到某话题上的消息。未授权访问导致攻击者能够在没有权限的情况下接收私密的信息，如空调状态，门锁状态等等，攻击者可能根据这些信息可以判断房间里是否有人。

H3 测试

H5 0x01测试环境

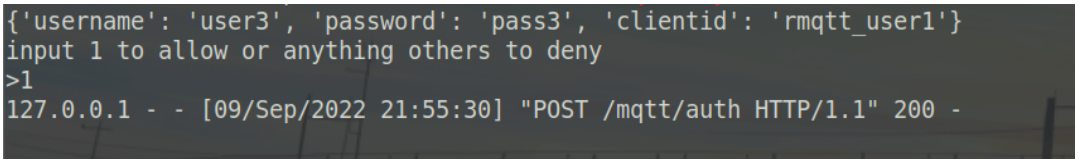
rmqtt v0.2.3

测试时使用rmqtt自带的rmqtt-auth-http插件

H5 0x02 测试步骤

- 受害者user1首先连接（clean start=false）到broker，并订阅testtopic，我们认为受害者具有连接权限和订阅权限，因此权限检查全部通过，两个http请求分别检查了连接与订阅（access: 1表示是订阅类型的访问）操作，全部允许

- 攻击者user3，通过使用与user1已经建立的连接相同的clientID（rmqtt_user1）申请连接（clean start=false）broker，可以在授权服务器上收到user3的连接授权申请，我们认为user3具有连接的权限，因此通过权限检查



- 正常设备user2连接到broker并向testtopic发布消息，我们认为user2具有连接和发布权限，因此权限检查通过，两个http请求分别检查了user2的连接权限和向testtopic写（access: 2表示是发布类型的访问，也即是发布消息）的权限

```
{'username': 'user2', 'password': 'pass2', 'clientid': 'rmqtt_user2'}
input 1 to allow or anything others to deny
>1
127.0.0.1 - - [09/Sep/2022 21:57:06] "POST /mqtt/auth HTTP/1.1" 200 -
{'username': 'user2', 'access': '2', 'ipaddr': '192.168.8.1', 'clientid': 'rmqtt_user2', 'topic': 'testtopic'}
input 1 to allow or anything others to deny
>1
127.0.0.1 - - [09/Sep/2022 21:57:21] "POST /mqtt/acl HTTP/1.1" 200 -
```

- 攻击者user3的连接收到user2发布的消息（但是user3不具有订阅权限）