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的权限和订阅某主题（如“testtopic”）的权限

01. 攻击者连接到broker，并订阅主题“testtopic”
02. 管理员撤销攻击者的订阅权限
03. 发布者（正常用户）向“testtopic”发布消息
04. 攻击者依然收到了broker转发的发布者的消息（即使攻击者的订阅权限已经被撤销）

0x02漏洞危害

攻击者能够在失去订阅权限之后仍然收到发布者发布到相关主题的消息。未授权访问可能导致攻击者在失去权限后仍然能收集一些私密的信息，比如获取空调状态、门锁状态，从而推断房间里有没有人。

测试

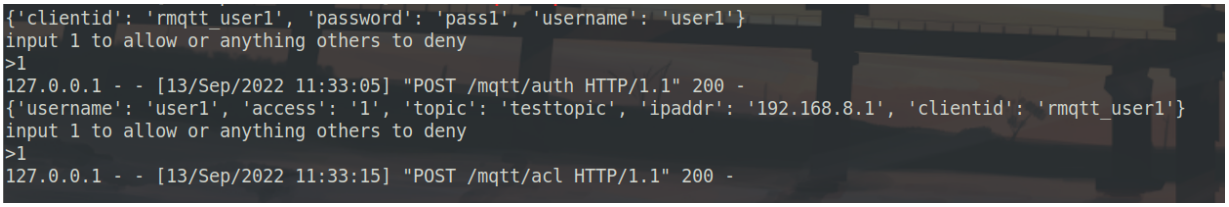
0x01测试环境

rmqtt v0.2.3

测试时使用rmqtt自带的rmqtt-auth-http插件

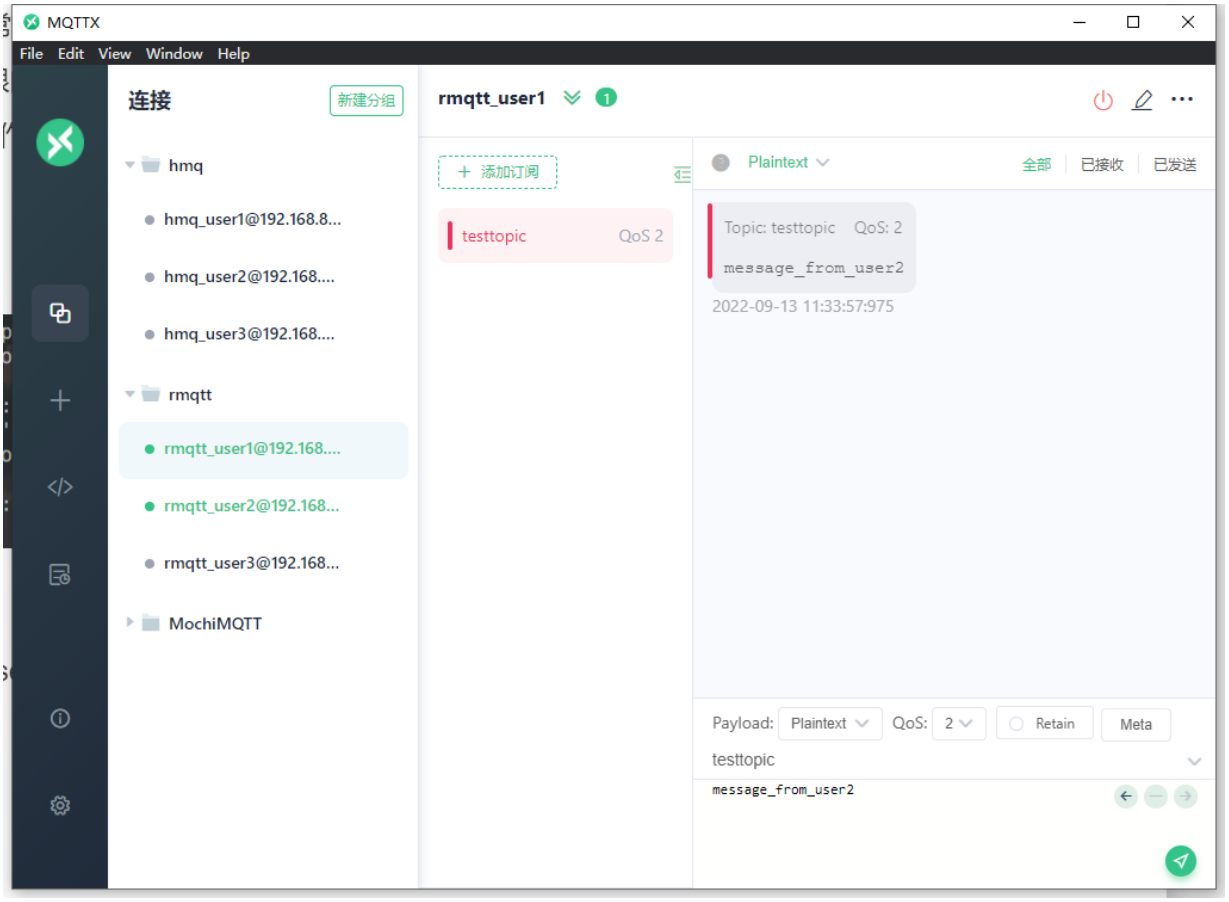
0x02测试步骤

- user1的客户端（作为攻击者）连接到broker，我们认为user1具有连接权限，因此通过发送状态码为200的http响应来表示允许连接。user1连接后订阅“testtopic”，此时我们认为user1具有订阅权限，因此通过发送状态码为200的http响应来允许订阅



- 之后我们撤销user1的订阅权限，具体行为是：当后续授权服务器再收到user1的订阅请求时，发送401状态码的http响应。
- 再使用user2（表示正常客户端）发起另一个连接，连接后向“testtopic”发布消息，可以看到授权服务器上收到了user2的申请发布权限的http请求，access: 2表示访问操作为发布操作，topic: stesttopic表示要访问的话题，user: user2表示进行操作的用户。我们认为user2具有发布权限，因此发送状态码为200的http响应表示允许发布

- 在此之后user1收到了user2发布的消息（此时我们认为user1已经不具有订阅权限）


MQTTX
File Edit View Window Help
连接
新建分组
hmq
hmq_user1@192.168.8...
hmq_user2@192.168....
hmq_user3@192.168....
rmqtt
rmqtt_user1@192.168....
rmqtt_user2@192.168...
rmqtt_user3@192.168...
MochiMQTT
rmqtt_user1
1
添加订阅
testtopic
QoS 2
Plaintext
全部
已接收
已发送
Topic: testtopic QoS: 2
message_from_user2
2022-09-13 11:33:57:975
Payload:
Plaintext
QoS:
2
Retain
Meta
testtopic
message_from_user2