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以及向某话题（如“testtopic”）发布消息的权限。

01. 受害设备上线（clean start=false）并订阅话题“testtopic”
02. 攻击者先使得受害设备掉线（可能通过DoS攻击，或者在酒店公寓等场景下，攻击者可能直接将设备关机）
03. 攻击者连接到broker并向testtopic发布了一条QoS1/QoS2消息
04. 攻击者的发布权限被撤销（比如酒店顾客租约到期签出）

05. 受害者连接到broker（clean start=false）
06. 受害者收到broker转发的攻击者发布的消息（即使此时攻击者已经失去了发布权限）

0x02漏洞危害

攻击者能够在失去发布权限之后仍然向订阅者发送消息。未授权访问可能导致攻击者在租约到期退房之后，仍然能向智能门锁的控制话题发布解锁命令，打开智能门锁。

测试

0x01测试环境

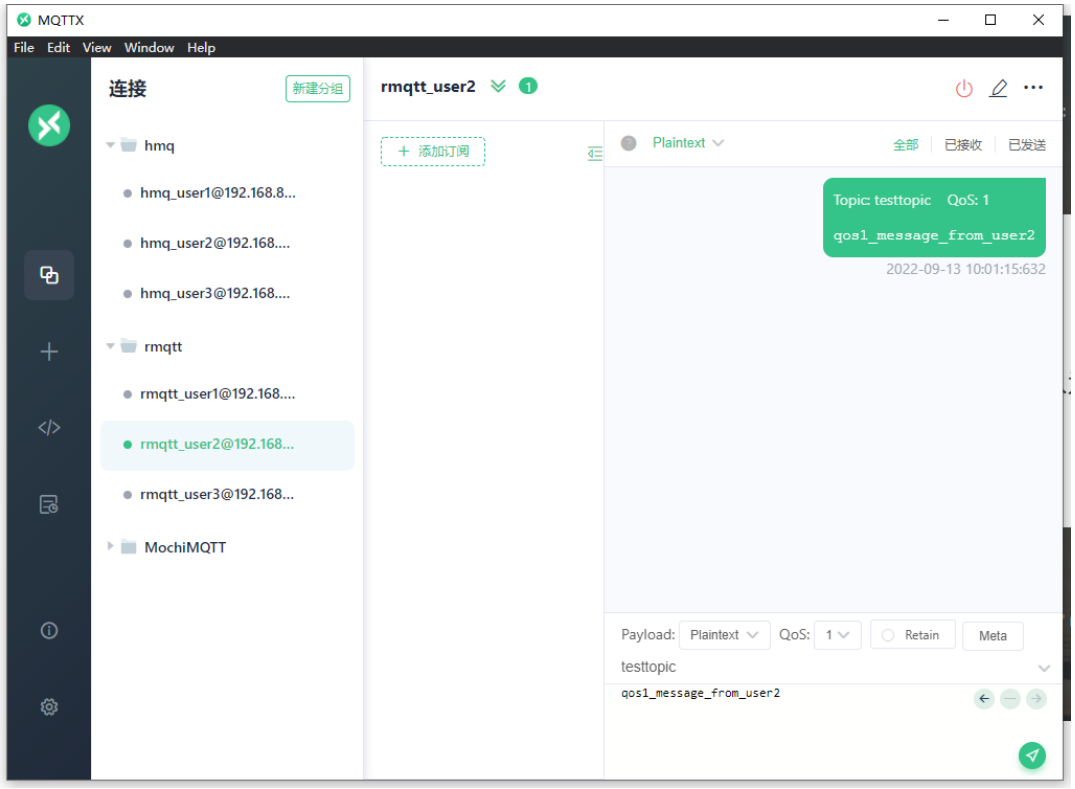
rmqtt v0.2.3

测试时使用rmqtt自带的rmqtt-auth-http插件

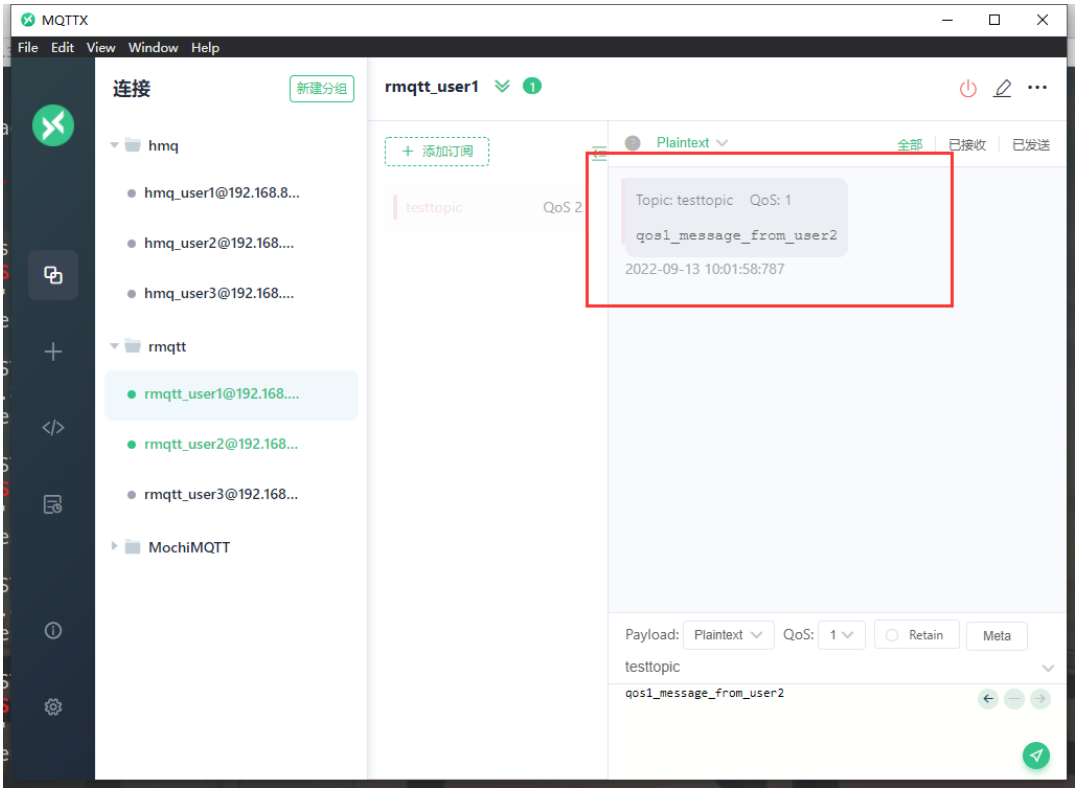
0x02 测试步骤1

- 用户user1模拟受害设备，首先使用clean start=false连接到broker并订阅“testtopic”，我们认为受害设备具有连接和订阅的权限，因此检查通过

- 为了模拟攻击者使得受害者设备掉线，可以直接让user1的连接断开
- user1断开连接后，攻击者user2连接到broker，并向testtopic发布一条QoS1消息，我们认为这时候攻击者的权限还没有被撤销，因此权限检查通过



- 之后我们撤销user2的发布权限，具体操作为：后续授权服务器收到任何user2请求发布的http请求时，全部拒绝
- 之后受害设备（clean start=false）重新连接到broker，然后收到了user2发布的消息（此时我们认为user2已经不具有发布权限了）

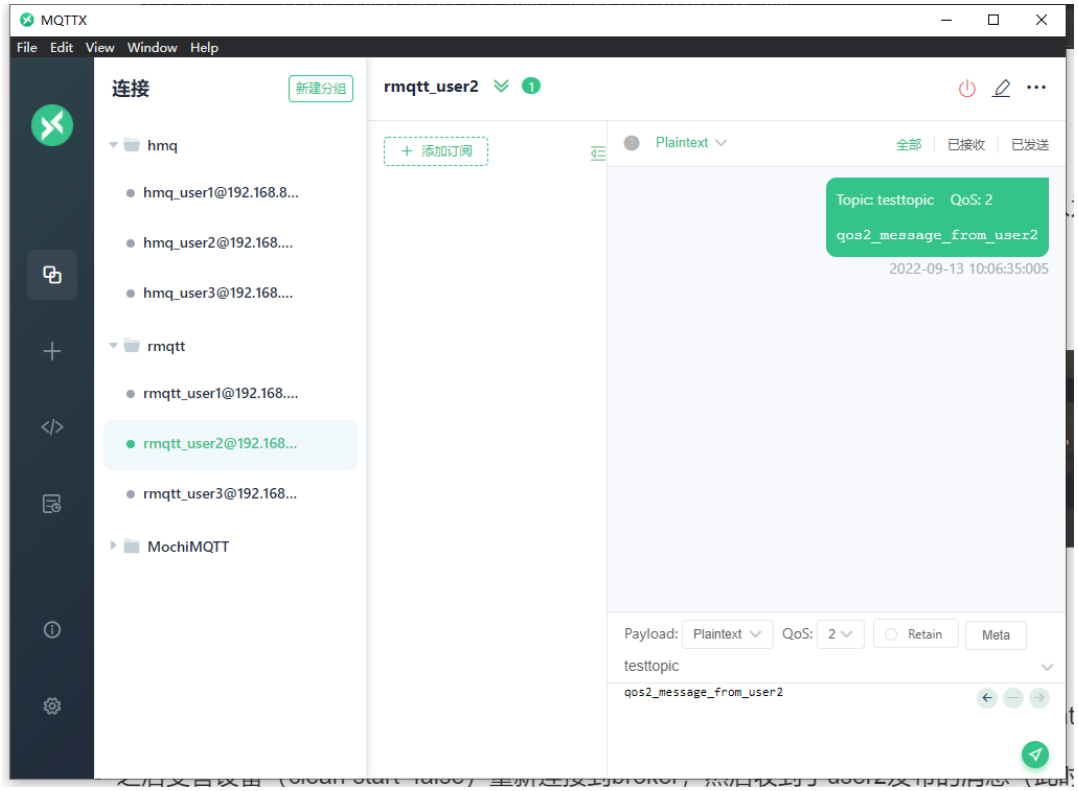


H5 0x03 测试步骤2

QoS2与QoS1类似，攻击者发布一条QoS2消息，broker将存储该消息，并且在重新投递时不检查发布者的权限

- 用户user1模拟受害设备，首先使用clean start=false连接到broker并订阅“testtopic”，我们认为受害设备具有连接和订阅的权限，因此检查通过

- 为了模拟攻击者使得受害者设备掉线，可以直接让user1的连接断开
- user1断开连接后，攻击者user2连接到broker，并向testtopic发布一条QoS2消息，我们认为这时候攻击者的权限还没有被撤销，因此权限检查通过



- 之后我们撤销user2的发布权限，具体操作为：后续授权服务器收到任何user2请求发布的http请求时，全部拒绝

- 之后受害设备（clean start=false）重新连接到broker，然后收到了user2发布的消息（此时我们认为user2已经不具有发布权限了）