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（发布者）连接到broker，连接时指定will topic为“testtopic”，并确定will message的payload
02. 智能设备订阅了相关主题（如“testtopic”）
03. 攻击者使用与受害者相同的clientID连接到broker，受害者的连接被断开

04. 智能设备收到了受害者的will message（由攻击者触发，但是攻击者并不具有发布权限）

H5 0x02漏洞危害

攻击者能够在没有发布权限的情况下向订阅者发布消息（时机取决于攻击者何时连接，消息内容和话题无法由攻击者控制）。未授权访问可能导致攻击者在没有发布权限的情况下，向智能门锁的控制话题发布解锁命令，打开智能门锁。

H3 测试

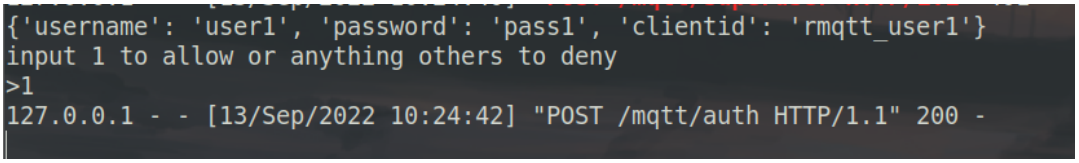
H5 0x01测试环境

rmqtt v0.2.3

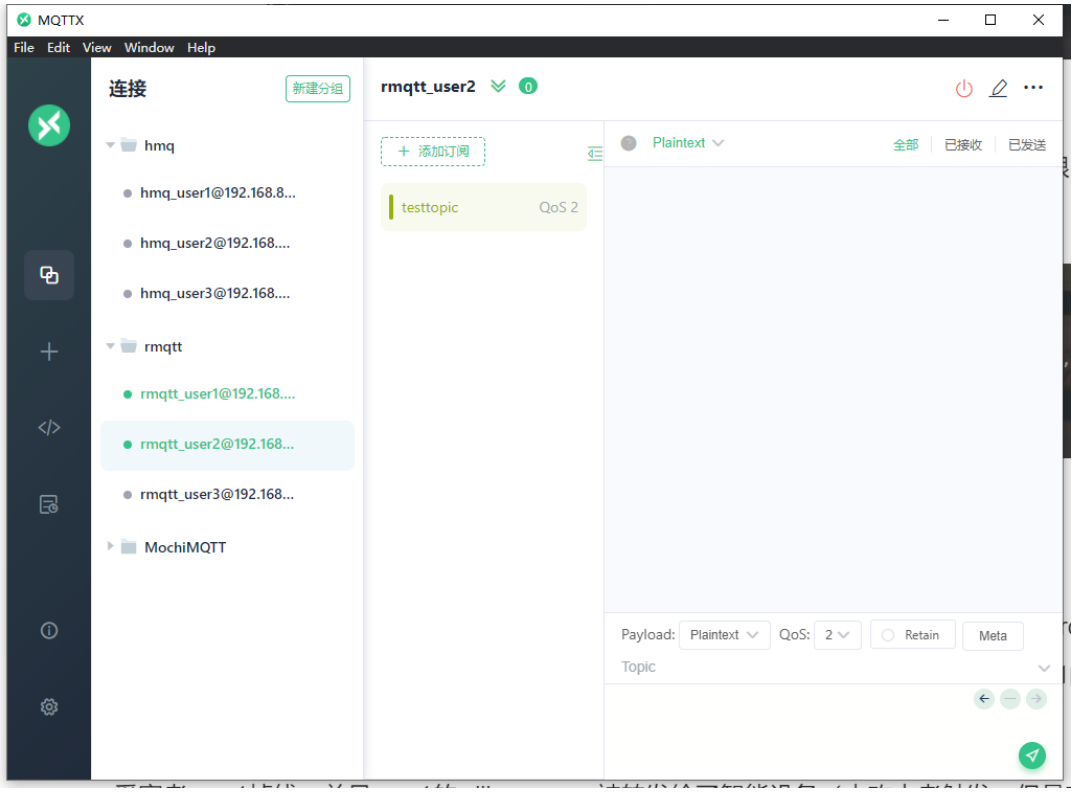
测试时使用rmqtt自带的rmqtt-auth-http插件

H5 0x02 测试步骤

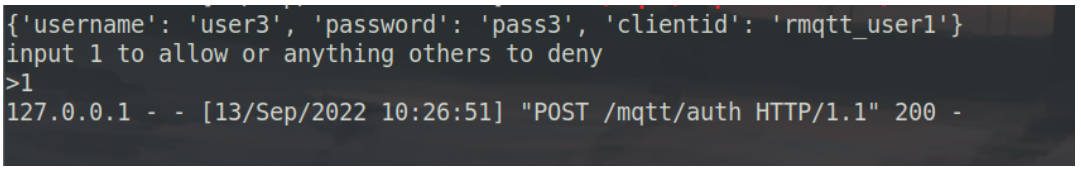
- 受害者user1首先连接到broker，并在连接时指定will topic为“testtopic”， will message payload为“unlock”，我们认为受害者具有连接权限和发布权限，因此权限检查通过，可以看到检查了user1的连接权限



- 智能设备user2连接到broker并订阅“testtopic”，我们认为智能设备具有链接权限和发布权限，因此检查通过



- 攻击者user3使用与受害者user1已经建立的连接相同的clientID（rmqtt_user1）连接到broker，我们认为攻击者具有连接权限（但没有发布权限），因此检查通过（这里即使检查不通过，user1的连接也会掉线，所以这里是一个条件极为宽松的dos攻击，攻击者只需要知道受害者的clientID即可，攻击者甚至不需要正确的账号和密码，只需要使用与受害者相同的clientID发送一个连接请求，无论攻击者是否连接成功，受害者都会被迫掉线），允许连接



- 受害者user1掉线，并且user1的will message被转发给了智能设备（由攻击者触发，但是攻击者不具有发布权限）