[FlashMQ(github)](https://github.com/halfgaar/FlashMQ)

注：我们已向厂商通报此安全问题及修复建议，并得到肯定回复

### 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）。

##### 0x01攻击场景

首先，攻击者暂时（作为租客）拥有主题“A”的权限。

1. 攻击者连接 FlashMQ Broker
2. 攻击者连接到broker，并且连接时指定will topic为“A”，payload为“bad will message”
3. 攻击者的发布权限被管理员或设备所有者撤销。
4. 智能设备上线并订阅了话题“A”
5. 攻击者客户端可以按照自己的期望，在指定时间直接切断自己和broker的网络连接（伪装异常掉线），此时broker认为攻击者的客户端异常掉线，将攻击者的will message投递给了智能设备

##### 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布消息（时机取决攻击者何时切断网络连接）。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

MQTT Broker：FlashMQv0.9.9，使用内置的、默认的、基于配置文件的认证和访问控制插件

配置文件如下：

* flashmq.conf

# File with usernames and hashed passwords compatible with Mosquitto.  
# You can use Mosquitto's mosquitto\_passwd to manage the file.  
mosquitto\_password\_file /etc/flashmq/mosquitto\_passwd\_file  
  
# ACL (access control lists) for users, anonymous users and patterns expandable  
# with %u (username) and %c (clientid). Format is Mosquitto's acl\_file.  
mosquitto\_acl\_file /etc/flashmq/mosquitto\_acl\_file  
  
allow\_anonymous false

* mosquitto\_passwd\_file

testuser:$6$Q1K0+7KCGstdgT5Z$/VKQTqy3B+Pqx0H3O+4QxYOCwavyH6xyXRxhW5y2zRioH8bDbJYmtO9c+fe8AoDLVRLbyvCe82V8pZIe/yWOPg==  
testuser2:$6$qscL9PY3fZNw9qSL$rln3IvA0bonpMhmJe3RPMDCQvRGmw0QXBI32GvPJwcN2qFyKfC32Bzt0/dZ+Cv9pCgCBfEecWhjgI25uL89ogQ==

* mosquitto\_acl\_file

user testuser  
topic write testtopic  
  
user testuser2  
topic read testtopic

MQTT Client：任意客户端，比如[MQTTX](https://mqttx.app/zh)

##### 0x02测试步骤

1. 配置完成后testuser2拥有订阅testtopic的权限，testuser拥有向testtopic发布消息的权限
2. testuser的客户端连接到broker并且在连接时指定will topic为“testtopic”（will message的payload取决于攻击者的意愿，比如“unlock”）
3. 管理员修改配置文件，撤销testuser的发布权限
4. testuser2的客户端连接到broker并订阅testtopic主题
5. testuser主动关闭自己的网络连接，此时broker认为testuser的客户端异常掉线，将其will message投递给了订阅者（testuser2的客户端）（即使此时testuser已经失去了发布权限）