**国家信息安全漏洞共享平台(CNVD)漏洞通报**

**关于Emitter Distributed Publish-Subscribe Platform存在未授权访问漏洞的情况通报**

国家互联网应急中心（CNCERT） 2022年07月07日

**漏洞描述**

[Emitter: Scalable Real-Time Communication Across Devices](https://emitter.io/)

[emitter-io/emitter: High performance, distributed and low latency publish-subscribe platform. (github.com)](https://github.com/emitter-io/emitter)

注：我们已向厂商通报此安全问题及修复建议

#### 0x01 攻击场景与测试

考虑IoT应用的共享场景，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，也就是房主  
可以授权其他普通用户（例如，Airbnb 客人）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和到期。我们  
认为管理员和设备是良性的，而客人可能是恶意的，会尽可能地去试图未授权访问设备（越权或是维持被撤销的权限）。

* **攻击场景**

首先，攻击者登记入住，因此目前攻击者拥有主题/通道“test”的 "read" 权限，可以暂时收到来自 "test" 的消息。  
  
  
1. 攻击者订阅channel "test"  
  
```  
 emitter.subscribe({  
 key: "<channel key>",  
 channel: "test"  
 });  
```  
  
2. 攻击者权限被撤销(`keyban`)  
  
3. 攻击者保持连接不断开  
  
4. 攻击者能够继续收到来自 "test" 的消息

* **漏洞危害**

攻击者可以在退房后继续监听设备消息或是接收其他敏感信息。

#### 0x02 漏洞测试步骤

* **测试环境**

**Emitter**: 3.0

**mqtt client**: https://github.com/emitter-io/python

**访问控制**: 内置keygen, keyban (在doc中未描述keyban，但在broker中已实现)

[Message Filtering - Emitter Documentation, Samples and Tutorials](https://emitter.io/develop/message-filtering/)

配置测试用户：

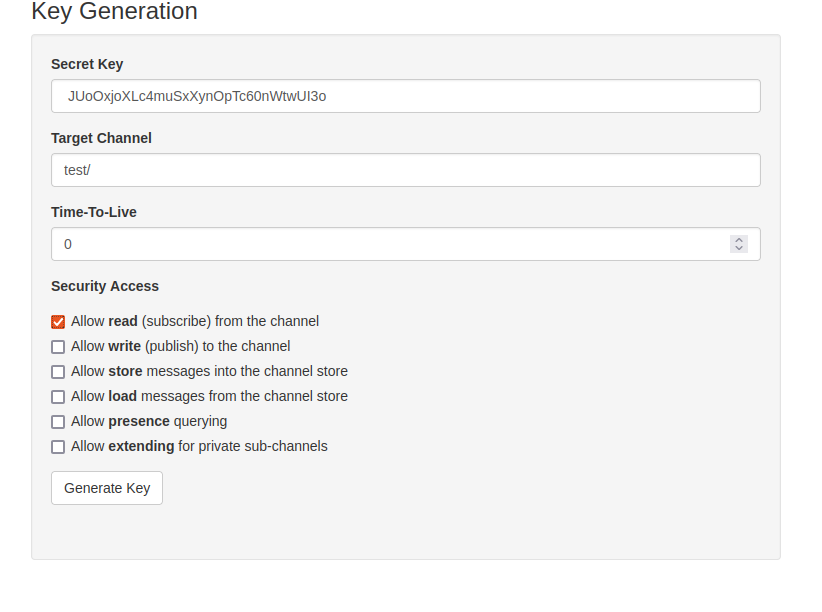
admin: 拥有所有权限

attacker: 拥有read权限

1. 首先按照文档指引，配置license ([emitter-io/emitter: High performance, distributed and low latency publish-subscribe platform. (github.com)](https://github.com/emitter-io/emitter))

[service] unable to find a license, make sure 'license' value is set in the config file or EMITTER\_LICENSE environment variable  
[service] generated new license: uppD0PFIcNK6VY-7PTo7uWH8EobaOGgRAAAAAAAAAAI  
[service] generated new secret key: JUoOxjoXLc4muSxXynOpTc60nWtwUI3o

1. 重启后创建一个channel key，作为"test" topic的密钥，并分配 "read" 权限，分发给attacker，通过访问 **http://127.0.0.1:8080/keygen**



1. 同理创建"test" 通道另一个admin key，让其拥有所有权限。
2. 如何撤销权限

使用官方[python sdk](https://github.com/emitter-io/python)的keyban功能可能存在无法成果撤销的情况，可使用下面的脚本（clientID不重要，主要是配置secret key以及target key）

def pubKeyBan():  
 client = mqtt.Client(client\_id="user1123", protocol=mqtt.MQTTv311)  
 #client.username\_pw\_set(username="user1", password="pass1")  
 client.on\_connect = connect\_callback\_v3  
  
 try:  
 conProperty = p.Properties(PacketTypes.PacketTypes.CONNECT)  
 pubProperty = p.Properties(PacketTypes.PacketTypes.PUBLISH)  
 client.connect(host="192.168.179.128", port=8080, keepalive=1000)  
 client.loop\_start()  
 while (input() != "xxx"):  
 request = {"secret": "D8qiQ2kOHD5b3xth2\_xtOsCs7Mjl2aUZ", "target": "P1-LbZvpKvYk7Fzu1nSXvT3Y20Rl5W09", "banned": False}  
 client.publish(topic="emitter/keyban/", payload=json.dumps(request), qos=0, retain=True)  
 except Exception as e:  
 print(e)  
 client.disconnect()

* **测试步骤**

1. 攻击者订阅channel "test"。

emitter.subscribe({  
 key: "<channel key>",  
 channel: "test"  
 });

1. 攻击者权限被撤销(keyban)。
2. 攻击者保持连接不断开。
3. 攻击者能够继续收到来自 "test" 的消息。

emitter.publish({  
 key: "<channel key>",  
 channel: "test",  
 message: "hello, emitter!"  
});

**关于CNVD**

国家信息安全漏洞共享平台（China National Vulnerability Database，简称CNVD）是由CNCERT联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的国家网络安全漏洞库，致力于建立国家统一的信息安全漏洞收集、发布、验证、分析等应急处理体系。

**关于CNCERT**

国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文简称是CNCERT或CNCERT/CC），成立于2002年9月，为非政府非盈利的网络安全技术中心，是我国计算机网络应急处理体系中的牵头单位。

作为国家级应急中心，CNCERT的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，维护国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82991537