**国家信息安全漏洞共享平台(CNVD)漏洞通报**

**关于Eclipse Mosquitto MQTT message Broker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05月28日

## 漏洞描述

[eclipse/mosquitto: Eclipse Mosquitto - An open source MQTT broker (github.com)](https://github.com/eclipse/mosquitto)

注：我们已向厂商通报此安全问题

#### 0x01 攻击场景

* **攻击场景**

首先，攻击者通过猜测或是受害者泄露得到了受害者的clientID，并且攻击者是一个无权限的状态  
1. 攻击者使用相同的clientID，并且以“Clean Start = False”连接broker。  
  
2. broker会触发take over机制，将已存在的受害者session踢下线，并且将受害者session中保存的(1. 订阅关系；2. 未完成的消息)保存到新的session中。  
  
3. broker随后触发受害者的will message。  
  
4. 恶意的will message被投递到订阅者。

* **漏洞危害**

1. 攻击者能继承受害者的订阅关系，如果拥有某些topic的read权限，便能直接收取消息，而无需subscribe权限去订阅topic
2. DoS攻击，将相同clientID的受害者踢下线
3. 恶意的will message，虽然攻击者无法控制will message的内容，但是能选择触发该will message的时机，并且攻击者本身对于该will message没有权限，是一种越权行为。

#### 0x02 漏洞测试步骤

* **测试环境**

**mosquitto**: 2.0.14

**mqtt client**: 任意客户端即可(这里测试使用mosquitto自带客户端)

**访问控制插件**: 官方插件[dynsec](https://mosquitto.org/documentation/dynamic-security/)，配置文件如下, 创建了两个role

admin: 拥有所有权限

attacker: 没有权限

{  
 "defaultACLAccess": {  
 "publishClientSend": false,  
 "publishClientReceive": true,  
 "subscribe": false,  
 "unsubscribe": true  
 },  
 "clients": [{  
 "username": "admin-user",  
 "textname": "Dynsec admin user",  
 "roles": [{  
 "rolename": "admin"  
 }],  
 "password": "Kmk6bi/ZwSLDHp9sveiiKPGytxy1f1/VFVEF8JwZdpdSLg5IZjshMDANkNwWOYE8Ii+iIFX5ogSdcHtx3aehEw==",  
 "salt": "cWjrh5nu7nMC3vfI",  
 "iterations": 101  
 }, {  
 "username": "user1",  
 "roles": [{  
 "rolename": "attacker",  
 "priority": 1000  
 }],  
 "password": "rDEjWxg9x2qjCWRGO63xVxFbSmZ38F8GyjrGKF6H30jAANRauc0/BBbYuf5pDLdvkxaWJA2h0oUsnBYVpozc/w==",  
 "salt": "4P4fvBDU7rxqHpxC",  
 "iterations": 101  
 }],  
 "groups": [],  
 "roles": [{  
 "rolename": "admin",  
 "acls": [{  
 "acltype": "publishClientSend",  
 "topic": "$CONTROL/dynamic-security/#",  
 "priority": 0,  
 "allow": true  
 }, {  
 "acltype": "publishClientSend",  
 "topic": "#",  
 "priority": 0,  
 "allow": true  
 }, {  
 "acltype": "publishClientReceive",  
 "topic": "$CONTROL/dynamic-security/#",  
 "priority": 0,  
 "allow": true  
 }, {  
 "acltype": "publishClientReceive",  
 "topic": "$SYS/#",  
 "priority": 0,  
 "allow": true  
 }, {  
 "acltype": "publishClientReceive",  
 "topic": "#",  
 "priority": 0,  
 "allow": true  
 }, {  
 "acltype": "subscribePattern",  
 "topic": "$CONTROL/dynamic-security/#",  
 "priority": 0,  
 "allow": true  
 }, {  
 "acltype": "subscribePattern",  
 "topic": "$SYS/#",  
 "priority": 0,  
 "allow": true  
 }, {  
 "acltype": "subscribePattern",  
 "topic": "#",  
 "priority": 0,  
 "allow": true  
 }, {  
 "acltype": "unsubscribePattern",  
 "topic": "#",  
 "priority": 0,  
 "allow": true  
 }]  
 }, {  
 "rolename": "attacker",  
 "acls": []  
 }]  
}

可使用[指导文档](https://mosquitto.org/documentation/dynamic-security/)中的方法创建role以及clients:

mosquitto\_ctrl dynsec init path/to/dynamic-security.json admin-user  
mosquitto\_ctrl -u admin-user dynsec createRole user

在mosuqitto中配置文件中配置使用该插件:

plugin path/to/mosquitto\_dynamic\_security.so  
plugin\_opt\_config\_file path/to/dynamic-security.json

* **测试步骤**

1. 观察者登录（admin）

clientID: "inspector"

订阅topic: "test"

$ mosquitto\_sub -u admin-user -P admin-password -t "test"

1. 受害者登录 (admin)

clientID: "cid"

will message: "mywill"

will topic: "test"

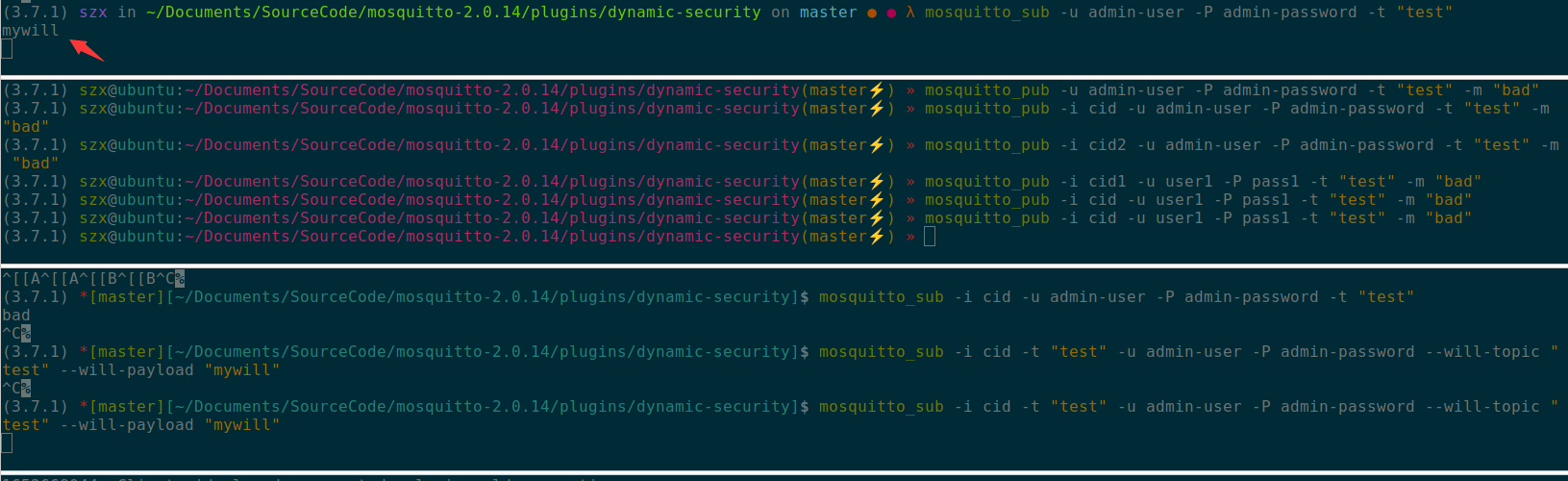
$ mosquitto\_sub -i cid -t "test" -u admin-user -P admin-password --will-topic "test" --will-payload "mywill"

1. 攻击者登录 (attacker)

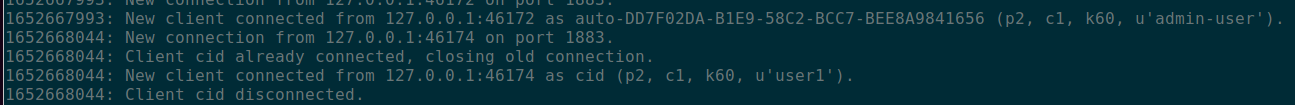
clientID: "cid"

$ mosquitto\_pub -i cid -u user1 -P pass1 -t "test" -m "bad"

可以看到，受害者被挤下线，并且触发了其will message



观察mosquitto日志，可以发现take over动作：



#### 0x03 漏洞原理分析

1. broker在收到一个CONNECT请求时，并且其clientID已经拥有了一个已存在的session，会无条件关闭已存在的session

src/handle\_connect.c: 208

session\_expiry\_\_remove(found\_context);  
 will\_delay\_\_remove(found\_context);  
 will\_\_clear(found\_context);  
  
 found\_context->clean\_start = true;  
 found\_context->session\_expiry\_interval = 0;  
 mosquitto\_\_set\_state(found\_context, mosq\_cs\_duplicate);  
 do\_disconnect(found\_context, MOSQ\_ERR\_SUCCESS);

1. 在take over时，未验证当前新session的权限，便将已存在session中的订阅关系恢复到新的session中

src/handle\_connect.c:167

for(i=0; i<context->sub\_count; i++){  
 if(context->subs[i]){  
 leaf = context->subs[i]->hier->subs;  
 while(leaf){  
 if(leaf->context == found\_context){  
 leaf->context = context;  
 }  
 leaf = leaf->next;  
 }  
  
 if(context->subs[i]->shared){  
 leaf = context->subs[i]->shared->subs;  
 while(leaf){  
 if(leaf->context == found\_context){  
 leaf->context = context;  
 }  
 leaf = leaf->next;  
 }  
 }  
 }  
 }

1. 在投递will message时，验证了will message的所有者的发布权限，导致will message被无权限的攻击者触发

src/handle\_connect.c:198

这里是take over导致触发will message的地方

if((found\_context->protocol == mosq\_p\_mqtt5 && found\_context->session\_expiry\_interval == 0)  
 || (found\_context->protocol != mosq\_p\_mqtt5 && found\_context->clean\_start == true)  
 || (context->clean\_start == true)  
 ){  
  
 context\_\_send\_will(found\_context);  
 }

=>

src/context.c:176

void context\_\_send\_will(struct mosquitto \*ctxt)  
{  
 if(ctxt->state != mosq\_cs\_disconnecting && ctxt->will){  
 if(ctxt->will\_delay\_interval > 0){  
 will\_delay\_\_add(ctxt);  
 return;  
 }  
  
 if(mosquitto\_acl\_check(ctxt,  
 ctxt->will->msg.topic,  
 (uint32\_t)ctxt->will->msg.payloadlen,  
 ctxt->will->msg.payload,  
 (uint8\_t)ctxt->will->msg.qos,  
 ctxt->will->msg.retain,  
 MOSQ\_ACL\_WRITE) == MOSQ\_ERR\_SUCCESS){  
  
 /\* Unexpected disconnect, queue the client will. \*/  
 db\_\_messages\_easy\_queue(ctxt,  
 ctxt->will->msg.topic,  
 (uint8\_t)ctxt->will->msg.qos,  
 (uint32\_t)ctxt->will->msg.payloadlen,  
 ctxt->will->msg.payload,  
 ctxt->will->msg.retain,  
 ctxt->will->expiry\_interval,  
 &ctxt->will->properties);  
 }  
 }  
 will\_\_clear(ctxt);  
}

**关于CNVD**

国家信息安全漏洞共享平台（China National Vulnerability Database，简称CNVD）是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信息安全漏洞信息共享知识库，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，是我国网络安全应急体系的核心协调机构。

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](mailto:vreport@cert.org.cn)

电话：010-82991537