Redis未授权访问漏洞分析

Redis 4.x/5.x 未授权访问漏洞

漏洞原理

Redis 默认情况下，会绑定在 0.0.0.0:6379，如果没有进行采用相关的策略，比如添加防火墙规则避免其他非信任来源 ip 访问等，这样将会将 Redis 服务暴露到公网上，如果在没有设置密码认证（一般为空）的情况下，会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，利用 Redis 自身的提供的config 命令，可以进行写文件操作，攻击者可以成功将自己的ssh公钥写入目标服务器的 /root/.ssh 文件夹的authotrized_keys 文件中，进而可以使用对应私钥直接使用ssh服务登录目标服务器。

Redis未授权访问在4.x/5.0.5以前版本下，我们可以使用master/slave模式加载远程模块，通过动态链接库的方式执行任意命令。

影响版本

数据库版本在 4.x / 5.x 以下。

靶场环境

```
http://download.redis.io/releases/
搭建 4.0.8
wget http://download.redis.io/releases/redis-4.0.8.tar.gz
tar -zxvf redis-4.0.8.tar.gz
cd redis-4.0.8
Make
Make test
配置更改
搭建好后外部无法连接，修改配置文件
注释掉绑定ip：bind 127.0.0.1   或者bind 0.0.0.0
Redis默认不是以守护进程的方式运行，可以通过该配置项修改，使用yes启用守护进程，设置为yes：
daemonize yes
保护模式,关闭保护模式，否则外部ip无法连接：protected-mode no
靶场防火墙开启6379端口
 firewall-cmd --list-ports
 firewall-cmd --zone=public --add-port=6379/tcp --permanent
 firewall-cmd --reload
redis-cli -h host -p port -a password
```

漏洞分析

简单的说，漏洞产生条件有以下两点：

redis绑定在 0.0.0.0:6379，且没有进行添加防火墙规则避免其他非信任来源ip访问等相关安全策略，直接暴露在公网；

没有设置密码认证（一般为空），可以免密码远程登录redis服务。

漏洞危害：

攻击者无需认证访问到内部数据，可能导致敏感信息泄露，黑客也可以恶意执行flushall来清空所有数据；

攻击者可通过EVAL执行lua代码，或通过数据备份功能往磁盘写入后门文件；
最严重的情况，如果Redis以root身份运行，黑客可以给root账户写入SSH公钥文件，直接通过SSH登录受害服务器

预防措施：
Redis添加密码验证；
更改端口（与其他服务不冲突）；
Redis尽量不要在公网开放（限制来源IP）；
使用高版本的Redis；