Redis未授权访问漏洞

更新时间：2017-01-06 12:09:40

一.漏洞描述

Redis因配置不当可以导致未授权访问，被攻击者恶意利用。当前流行的针对Redis未授权访问的一种新型攻击方式，在特定条件下，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，可导致服务器权限被获取和数据删除、泄露或加密勒索事件发生，严重危害业务正常服务。

二.Redis安全漏洞影响

一旦入侵成功，Redis数据会丢失，攻击者可直接添加账号用于ssh远程登录控制服务器，会给用户的 Redis 运行环境以及 Linux 主机造成安全风险，引发重要数据删除、泄露或加密勒索事件发生。

三.已确认被成功利用的软件及系统

使用redis客户端直接无账号成功登录redis：

```
1. `root@kali:~# redis-cli -h 10.16.10.2
2. redis 10.16.10.2:6379&gt; keys *
3. 1) "1"`
```

从登录的结果可以看出该redis服务对公网开放，且未启用认证。

三.建议修复方案

- **网络层加固**

1.指定redis服务使用的网卡（需要重启redis才能生效）redis默认是监听的127.0.0.1上，如果仅仅是本地通信，请确保监听在本地。这种方式缓解了redis的风险，当然并不能绝对保证安全了，假如攻击者有了一个webshell，并且redis以root用户运行，就可以通过该redis来反弹shell，来实现提权。

在 redis.conf 文件中找到 “# bind 127.0.0.1” ，把前面的#号去掉，然后保存。注：修改后只有本机才能访问Redis，也可以指定访问源IP访问Redis。

```
1. # bind 192.168.1.100 10.0.0.1
```

2.设置防火墙策略如果正常业务中Redis服务需要被其他服务器来访问，可以设置iptables策略仅允许指定的IP来访问Redis服务。

```
1. iptables -A INPUT -s x.x.x.x -p tcp --dport 6379 -j ACCEPT
```

- **账号与认证**

1.设置访问密码（需要重启redis才能生效）在 redis.conf 中找到“requirepass”字段，在后面填上你需要的密码，Redis客户端也需要使用此密码来访问Redis服务。

打开/etc/redis/redis.conf配置文件:

```
1.  #requirepass !QE%^E3323BDWEwwwe1839
```

确保密码的复杂度，配置完毕后重启服务即可生效。

- **服务运行权限最小化**

1.修改Redis服务运行账号（需要重启redis才能生效）请以较低权限账号运行Redis服务，并禁用该账号的登录权限。以下为创建一个无home目录和无法登陆的普通权限账号：

```
1. #useradd -M -s /sbin/nologin [username]
```

- **服务精细化授权**

redis没有权限分离之说，无管理员账号和普通账户之分，导致攻击者登陆后可执行任意操作，因此需要隐藏重要命令，具体如下：

FLUSHDB, FLUSHALL, KEYS,PEXPIRE, DEL, CONFIG, SHUTDOWN, BGREWRITEAOF, BGSAVE, SAVE, SPOP, SREM, RENAME,DEBUG, EVAL 等。

在redis2.8.1 及 redis3.x(<3.0.2) 版本下存在eval沙箱逃逸漏洞，攻击者可通过该漏洞执行任意Lua代码。

具体缓解攻击操作，供参考：下述配置将config/flushdb/flushall设置为空，即禁用该命令；也可命名一些攻击者难以猜解的名字。

rename-command CONFIG “”

rename-command flushall “”

rename-command flushdb “”

rename-command shutdown shotdown_test

保存后，执行/etc/init.d/redis-server restart重启生效。

- **安全补丁**

不定期关注最新软件版本，并升级redis到最新版，防止新漏洞被利用。