



Redis主从复制RCE影响分析

山石网科

2022-03-16 10:08:45

226308

所在地 广东省

Redis 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
OK
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offset，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

文章目录

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

浏览更多



