Redis基线检查

禁止使用root用户启动 | 访问控制

描述

使用root权限去运行网络服务是比较有风险的（nginx和apache都是有独立的work用户，而redis没有）。redis crackit 漏洞就是利用root用户的权限来替换或者增加authorized_keys，来获取root登录权限的

加固建议

使用root切换到redis用户启动服务:
useradd -s /sbin/nologin -M redis
-s<shell> 指定用户登入后所使用的shell。
-M 不要自动建立用户的登入目录
sudo -u redis /<redis-server-path>/redis-server /<configpath>/redis.conf

禁止监听在公网 | 访问控制

描述

Redis监听在0.0.0.0，可能导致服务对外或内网横向移动渗透风险，极易被黑客利用入侵。

加固建议

在redis的配置文件redis.conf中配置如下：bind 127.0.0.1或者内网IP，然后重启redis
操作时建议做好记录或备份

打开保护模式 | 访问控制

描述

redis默认开启保护模式。要是配置里没有指定bind和密码，开启该参数后，redis只能本地访问，拒绝外部访问。

加固建议

redis.conf安全设置： # 打开保护模式protected-mode yes
操作时建议做好记录或备份

限制 redis 配置文件访问权限 | 文件权限

描述

因为redis密码明文存储在配置文件中，禁止不相关的用户访问改配置文件是必要的，设置redis配置文件权限为600

加固建议

执行以下命令修改配置文件权限：chmod 600 /<filepath>/redis.conf

修改默认6379端口 | 服务配置

描述

避免使用熟知的端口,降低被初级扫描的风险

加固建议

编辑文件redis的配置文件redis.conf，找到包含port的行，将默认的6379修改为自定义的端口号，然后重启redis
操作时建议做好记录或备份

禁用或者重命名危险命令 | 入侵防范

描述

Redis中线上使用keys *命令，也是非常危险的。因此线上的Redis必须考虑禁用一些危险的命令，或者尽量避免谁都可以使用这些命令，Redis没有完整的管理系统，但是也提供了一些方案。

加固建议

修改 redis.conf 文件，添加
rename-command FLUSHALL ""
rename-command FLUSHDB ""
rename-command CONFIG   ""
rename-command KEYS   ""
rename-command SHUTDOWN ""
rename-command DEL ""
rename-command EVAL ""
然后重启redis。 重命名为"" 代表禁用命令，如想保留命令，可以重命名为不可猜测的字符串，如： rename-command FLUSHALL joYAPNXRPmcarcR4ZDgC

开启 Redis 密码认证，并设置高度复杂度密码 | 身份鉴别

描述

redis在redis.conf配置文件中，设置配置项requirepass， 开户密码认证。 redis因查询效率高，auth这种命令每秒能处理9w次以上，简单的redis的密码极容易为攻击者暴破。

加固建议

打开redis.conf，找到requirepass所在的地方，修改为指定的密码，密码应符合复杂性要求：
- 长度8位以上
- 包含以下四类字符中的三类字符:
- 英文大写字母(A 到 Z)
- 英文小写字母(a 到 z)
- 10 个基本数字(0 到 9)
- 非字母字符(例如 !、$、%、@、^、&等，#除外)
- 避免使用已公开的弱密码，如：abcd.1234 、admin@123等
- 再去掉前面的#号注释符，然后重启redis

操作时建议做好记录或备份
中危-版本存在安全漏洞

Redis 以下版本存在漏洞 | 入侵防范

描述

Redis 2.8.1 之前版本和 3.0.2 之前 3.x 版本存在字节码命令执行漏洞
https://avd.aliyun.com/detail?id=AVD-2015-4335
Redis 4.x至5.0.5版本存在主从复制命令执行漏洞RCE
Redis 3.2.0 至 3.2.4 版本存在缓冲区溢出漏洞，可导致任意代码执行
https://avd.aliyun.com/detail?id=AVD-2016-8339

加固建议

更新服务至最新版本，完成漏洞的修复，这些漏洞基于未授权访问或者服务存在弱口令，完成访问认证加固可降低被入侵风险。