* 1. Redis数据库系统安全基线配置规范
     + 1. 启用密码认证

|  |  |
| --- | --- |
| 要求内容 | 在 redis.conf 中找到“requirepass”字段，查看是否已设置登陆密码，Redis客户端也需要使用此密码来访问Redis服务 |
| 操作指南 | 在 redis.conf 中找到“requirepass”字段  vi /etc/redis/redis.conf  requirepass 密码字段 |
| 检测方法 |  |

* + - 1. 监听地址限制

|  |  |
| --- | --- |
| 要求内容 | 在 redis.conf 文件中找到bind+IP字段，确保前面没有“#”，表示Redius限制了监听地址。 |
| 操作指南 | 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，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，如：  bind 192.168.1.100 10.0.0.1 |
| 检测方法 |  |

* + - 1. 端口限制

|  |  |
| --- | --- |
| 要求内容 | 检查是否设置防火墙策略，如果正常业务中Redis服务需要被其他服务器来访问，确保只有指定IP和端口才可以访问Redis服务。 |
| 操作指南 | 可以设置iptables策略仅允许指定的IP和端口来访问Redis服务：  iptables -A INPUT -s x.x.x.x -p tcp --dport 6379 -j ACCEPT。 |
| 检测方法 |  |

* + - 1. 权限最小化

|  |  |
| --- | --- |
| 要求内容 | 检查用户权限是否最小化。 |
| 操作指南 | 访谈管理员，梳理账号和权限列表，检查是否仅为用户分配了所需的最小权限。  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：  useradd -M -s /sbin/nologin [username] |
| 检测方法 |  |

* + - 1. 服务精细化授权

|  |  |
| --- | --- |
| 要求内容 | 检查是否配置了服务精细化授权。 |
| 操作指南 | 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。 |
| 检测方法 |  |

* + - 1. 设置redis安装目录权限

|  |  |
| --- | --- |
| 要求内容 | 设置redis的主目录权限为700。 |
| 操作指南 | 执行命令#ls -l $REDIS\_PATH查看安装目录的权限  执行#chmod 700 /etc/redis/redis.conf |
| 检测方法 |  |

* + - 1. 配置客户端闲置时间

|  |  |
| --- | --- |
| 要求内容 | 当客户端闲置多长时间后关闭连接，如果指定为0，表示关闭该功能。 |
| 操作指南 | 空闲时间设置为300  编辑redis配置文件vi $REDIS\_PATH\redis.conf增加timeout 300 |
| 检测方法 |  |

* + - 1. 安全补丁

|  |  |
| --- | --- |
| 要求内容 | 检查Redis是否为最新版本。 |
| 操作指南 | 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。 |
| 检测方法 |  |

* + - 1. 日志安全

|  |  |
| --- | --- |
| 要求内容 | 开启日志审计功能 |
| 操作指南 | 配置Redis.conf文件：  loglevel notice#日志等级  logfile "/usr/redis/log/redis.log"#日志保存路径 |
| 检测方法 |  |