# 漏洞修复

### 1 允许Traceroute探测

iptables -A INPUT -p ICMP --icmp-type time-exceeded -j DROP  
iptables -A OUTPUT -p ICMP --icmp-type time-exceeded -j DROP  
service iptables save

### 2 OpenSSH 命令注入漏洞(CVE-2020-15778)

**该漏洞复现简单，漏洞等级 严重。复现需要知道ssh密码，主要针对知道ssh密码却不给登录，这样就可进行反弹shell获取权限了。**

<https://blog.csdn.net/qq_42947816/article/details/122807007>

修复方法

#### 2.1 禁用scp,使用rsync

##### 方法一 删除openssh-clients

查询openssh版本，删除openssh-clients相关软件包

rpm -qa|grep openssh-\*

删除openssh-clients

yum remove openssh-clients -y  
或者  
rpm -e openssh-clients --nodeps #不删除依赖包

##### 方法二：移除scp执行权限

whereis scp #查找scp所在目录  
cd /usr/bin  
chmod -x scp #移除执行权限   
或者  
mv scp .scp.bak  
或者  
chmod 000 scp  
ll scp

方法三:将scp命令别名为空

alias scp="printf ''" //#the user won't be able to run thi

#### 2.2 SSH账密确保为强口令且周期性更换密码

#### 2.3 升级OpenSSH为最新版

<https://blog.csdn.net/qq_39595769/article/details/122406702>

<https://blog.csdn.net/ximenjianxue/article/details/111995636>

[瞒天过海-修改openssh版本号](https://blog.csdn.net/bigwood99/article/details/115374894?spm=1001.2101.3001.6661.1&utm_medium=distribute.pc_relevant_t0.none-task-blog-2%7Edefault%7ECTRLIST%7EPayColumn-1-115374894-blog-117549337.pc_relevant_3mothn_strategy_and_data_recovery&depth_1-utm_source=distribute.pc_relevant_t0.none-task-blog-2%7Edefault%7ECTRLIST%7EPayColumn-1-115374894-blog-117549337.pc_relevant_3mothn_strategy_and_data_recovery&utm_relevant_index=1)

### 3 OpenSSH 安全漏洞(CVE-2021-41617)

升级openssh到最新版本

### 4 OpenSSH 安全漏洞(CVE-2016-20012)

升级openssh到最新版本

<https://www.cnblogs.com/fivekills/p/16494677.html>

<http://www.cnnvd.org.cn/web/xxk/ldxqById.tag?CNNVD=CNNVD-202109-1073> 国家安全信息漏洞库

### 5 CentOS7-openssh漏洞修复方法（修改openssh版本号）