修复OpenSSH漏洞

友情提示：请阅读完文章，再进行操作，感谢支持，祝您万事胜意！

漏洞概括

- OpenSSH 输入验证错误漏洞(CVE-2019-16905)
- OpenSSH 命令注入漏洞(CVE-2020-15778)
- OpenSSH 安全漏洞(CVE-2021-28041)

一般线上用的云主机的ssh版本都还比较低;线上的云主机版本还处于OpenSSH_7.4p1。2021年来，云主机进行了漏洞扫描，出现了大量openssh的漏洞，我尝试升级过8.4、8.5的版本。由于8.5版本也有漏洞，这一次我们直接升级到OpenSSH_8.6p1。

```
[root@ncayu8847 ~]# ssh -V
OpenSSH_7.4p1, OpenSSL 1.0.2k-fips  26 Jan 2017
```

那我们开始升级吧！

你需要准备的

openssh安装包：

- openssh-8.6p1.tar.gz
- openssl-1.1.1h.tar.gz
- zlib-1.2.11.tar.gz

你可以把这三个文件放到到linux的一个文件夹里；然后进行解压，编译。

升级openssh的步骤

1.解压升级包

```
tar xzvf openssh-8.6p1.tar.gz

tar xzvf openssl-1.1.1h.tar.gz

tar xzvf zlib-1.2.11.tar.gz
```

2.编译安装zlib

```
cd zlib-1.2.11

./configure --prefix=/usr/local/zlib

make && make install
```

3.编译安装openssl

```
cd openssl-1.1.1g

./config --prefix=/usr/local/ssl -d shared

make && make install

echo '/usr/local/ssl/lib' >> /etc/ld.so.conf

ldconfig -v
```

4.安装openssh

```
cd openssh-8.6p1

./configure --prefix=/usr/local/openssh --with-zlib=/usr/local/zlib --with-ssl-dir=/usr/local/ssl

make && make install
```

5.sshd_config文件修改

```
echo 'PermitRootLogin yes' >>/usr/local/openssh/etc/sshd_config

echo 'PubkeyAuthentication yes' >>/usr/local/openssh/etc/sshd_config

echo 'PasswordAuthentication yes' >>/usr/local/openssh/etc/sshd_config
```

6.备份原有文件，并将新的配置复制到指定目录

```
mv /etc/ssh/sshd_config /etc/ssh/sshd_config.bak
cp /usr/local/openssh/etc/sshd_config /etc/ssh/sshd_config

mv /usr/sbin/sshd /usr/sbin/sshd.bak
cp /usr/local/openssh/sbin/sshd /usr/sbin/sshd

mv /usr/bin/ssh /usr/bin/ssh.bak
cp /usr/local/openssh/bin/ssh /usr/bin/ssh

mv /usr/bin/ssh-keygen /usr/bin/ssh-keygen.bak
cp /usr/local/openssh/bin/ssh-keygen /usr/bin/ssh-keygen

mv /etc/ssh/ssh_host_ecdsa_key.pub /etc/ssh/ssh_host_ecdsa_key.pub.bak
cp /usr/local/openssh/etc/ssh_host_ecdsa_key.pub /etc/ssh/ssh_host_ecdsa_key.pub
```

7.启动sshd

```
service sshd restart
```

8.查看信息版本

```
ssh -V
```

升级中遇到的问题

openssh的路径

路径一：Loaded: loaded (/etc/rc.d/init.d/sshd;

```
[root@localhost system]# systemctl status sshd.service
● sshd.service - SYSV: OpenSSH server daemon
   Loaded: loaded (/etc/rc.d/init.d/sshd; bad; vendor preset: enabled)
   Active: active (running) since Fri 2021-04-16 18:22:17 CST; 6 days ago
     Docs: man:systemd-sysv-generator(8)
  Process: 1948 ExecStop=/etc/rc.d/init.d/sshd stop (code=exited, status=0/SUCCESS)
  Process: 1957 ExecStart=/etc/rc.d/init.d/sshd start (code=exited, status=0/SUCCESS)
 Main PID: 1965 (sshd)
   CGroup: /system.slice/sshd.service
           ├─ 1965 sshd: /usr/sbin/sshd [listener] 0 of 10-100 startups
           ├─112343 sshd: root@pts/0,pts/1
           ├─112345 -bash
           ├─112362 sshd: root@notty
           ├─112364 -bash
           ├─112381 /usr/local/openssh/libexec/sftp-server
           ├─112388 /usr/local/openssh/libexec/sftp-server
           ├─112395 /usr/local/openssh/libexec/sftp-server
           ├─112402 /usr/local/openssh/libexec/sftp-server
           ├─112412 /usr/local/openssh/libexec/sftp-server
           ├─112427 /usr/local/openssh/libexec/sftp-server
           ├─112487 top
```

路径二：Loaded: loaded (/usr/lib/systemd/system/sshd.service;

```
[root@ncayu8847 ~]# ssh -V
OpenSSH_7.4p1, OpenSSL 1.0.2k-fips  26 Jan 2017
[root@ncayu8847 ~]# systemctl status sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)
   Active: active (running) since 一 2021-04-26 20:59:23 CST; 1 months 3 days ago
     Docs: man:sshd(8)
           man:sshd_config(5)
 Main PID: 1189 (sshd)
   CGroup: /system.slice/sshd.service
           └─1189 /usr/sbin/sshd -D

5月  29 23:54:28 ncayu8847 sshd[31069]: Did not receive identification string from 39.103.159.236 port 35100
5月  30 04:10:45 ncayu8847 sshd[31467]: Bad protocol version identification '\026\003\001\002' from 101.133.147.20 port 56700
5月  30 04:10:46 ncayu8847 sshd[31468]: Bad protocol version identification 'GET / HTTP/1.1' from 101.133.147.20 port 56732
5月  30 04:10:46 ncayu8847 sshd[31469]: Bad protocol version identification 'GET / HTTP/2' from 101.133.147.20 port 56756
5月  30 04:10:46 ncayu8847 sshd[31470]: Bad protocol version identification '\026\003\001\002' from 101.133.147.20 port 56782
5月  30 04:10:46 ncayu8847 sshd[31471]: Bad protocol version identification 'GET / HTTP/1.1' from 101.133.147.20 port 56798
5月  30 04:10:46 ncayu8847 sshd[31472]: Bad protocol version identification 'GET / HTTP/2' from 101.133.147.20 port 56820
5月  30 08:56:10 ncayu8847 sshd[31740]: Did not receive identification string from 209.17.97.42 port 65372
5月  30 09:33:59 ncayu8847 sshd[31775]: Accepted password for root from 116.237.140.20 port 61417 ssh2
5月  30 09:34:00 ncayu8847 sshd[31792]: Accepted password for root from 116.237.140.20 port 61418 ssh2
```

openssh有两种启动路径，

Loaded: loaded (/etc/rc.d/init.d/sshd;容易升级

Loaded: loaded (/usr/lib/systemd/system/sshd.service;升级之后sshd起不来了

如果你的sshd的启动路径是Loaded: loaded (/etc/rc.d/init.d/sshd;那么按照上面的步骤就可以升级成功了，但是如果你的sshd启动路径是Loaded: loaded (/usr/lib/systemd/system/sshd.service;就话需要进一步操作；把启动路径换成/etc/rc.d/init.d/sshd。

操作详情：

```
##从原先的解压包中拷贝一些文件到目标位置

cd openssh-8.6p1/contrib/redhat

cp -a sshd.init /etc/init.d/sshd

cp -a sshd.pam /etc/pam.d/sshd.pam

chmod +x /etc/init.d/sshd

chkconfig --add sshd

systemctl enable sshd
```

修改完配置，需要重新加载

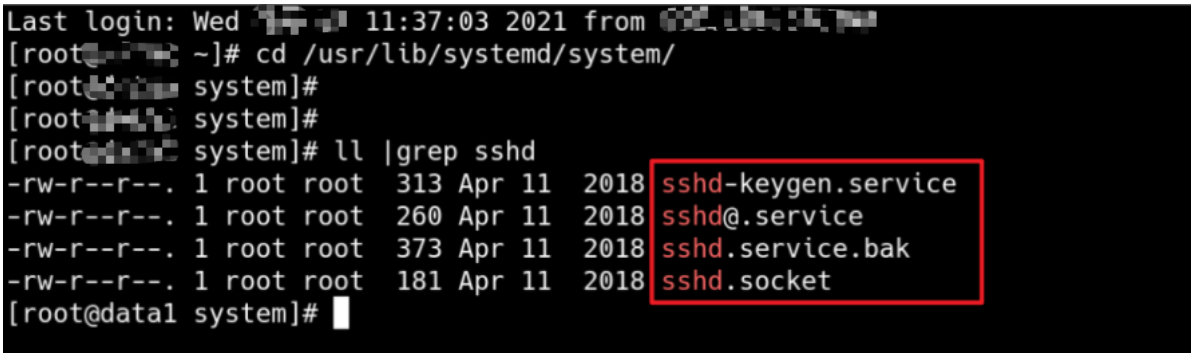
```
systemctl daemon-reload
```

如何变更成/etc/rc.d/init.d/sshd路径下启动

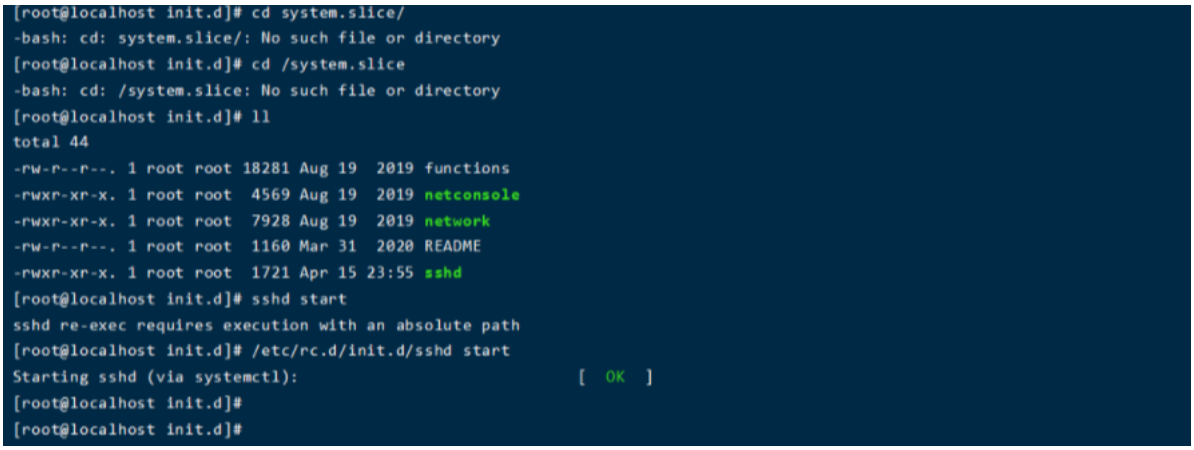
```
需要，进入到sshd.service的目录，然后先备份，再删除掉

cd /usr/lib/systemd/system/

ll |grep sshd
```



如何启动sshd程序




```
[root@localhost init.d]# ll
total 44
-rw-r--r--. 1 root root 18281 Aug 19  2019 functions
-rwxr-xr-x. 1 root root  4569 Aug 19  2019 netconsole
-rwxr-xr-x. 1 root root  7928 Aug 19  2019 network
-rw-r--r--. 1 root root  1160 Mar 31  2020 README
```

```
-rwxr-xr-x. 1 root root  1721 Apr 15 23:55 sshd
[root@localhost init.d]# sshd start
sshd re-exec requires execution with an absolute path  #sshd重新执行需要使用绝对路径执行
[root@localhost init.d]# /etc/rc.d/init.d/sshd start
Starting sshd (via systemctl):                             [  OK  ]
[root@localhost init.d]#
[root@localhost init.d]#
[root@localhost init.d]#
[root@localhost init.d]#
[root@localhost init.d]#
[root@localhost init.d]# systemctl status sshd
```

sshd启动方式

```
/etc/rc.d/init.d/sshd start  #启动sshd

/etc/rc.d/init.d/sshd stop   #停止sshd

#其他命令

systemctl enable sshd  #开机自动启动

systemctl start sshd   #启动sshd

systemctl status sshd   #查看状态

systemctl restart sshd  # 重新启动
```