

# 编译升级 OpenSSL、OpenSSH 版本

在对业务系统做漏洞扫描时，很多时候会出现 OpenSSL、OpenSSH 组件（以下简称组件）的安全漏洞隐患，需要通过升级新的版本来解决漏洞问题。本文介绍在内网环境下源码编译安装新版上述软件的方法。

需自行准备：FTP、HTTP 服务器软件，相关系统 iso 镜像包。

测试成功的 Linux 版本有：

- Red Hat Enterprise Linux Server release 6.6 (Santiago)
- CentOS 6.5 (Final)
- CentOS 6.10 (Final)
- Red Hat Enterprise Linux 7.3

其它 Linux 内核操作系统请自行评估测试！

**本次升级不涉及服务器重启。**

序号	漏洞名称	危险级别	主机数量	漏洞类型	CVE编号	存在主机
1	OpenSSH J-PAKE授权码漏洞(CVE-2010-4478)	严重	1	守护进程类	CVE-2010-4478	192.168.10.55
2	OpenSSH "hash_buffer" 缓冲区溢出漏洞(CVE-2014-1692)	严重	1	守护进程类	CVE-2014-1692	192.168.10.55
3	OpenSSH 远程拒绝服务漏洞(CVE-2010-5107)	高危	1	守护进程类	CVE-2010-5107	192.168.10.55
4	OpenSSH glob表达式拒绝服务漏洞(CVE-2010-4755)	高危	1	守护进程类	CVE-2010-4755	192.168.10.55
5	OpenSSH sshd_monitor文件权限许可和访问控制漏洞	高危	1	守护进程类	CVE-2015-6564	192.168.10.55
6	OpenSSH数字错误漏洞(CVE-2011-5000)	高危	1	守护进程类	CVE-2011-5000	192.168.10.55
7	OpenSSH auth_parse_options函数信任管理漏洞(CVE-2012-0814)	高危	1	守护进程类	CVE-2012-0814	192.168.10.55
8	OpenSSH 信息泄露漏洞(CVE-2011-4327)	高危	1	守护进程类	CVE-2011-4327	192.168.10.55
9	OpenSSH sshd_monitor组件输入验证漏洞(CVE-2015-6563)	高危	1	守护进程类	CVE-2015-6563	192.168.10.55
10	ssh_检测漏洞和版本	中危	1	守护进程类	--	192.168.10.55
11	ssh_协议版本	中危	1	守护进程类	--	192.168.10.55
12	SSH信息获取	中危	1	信息收集类	CVE-1999-0634	192.168.10.55
13	ICMP端口扫描获取	中危	1	信息收集类	CVE-1999-0524	192.168.10.55
14	RPCBIND/PORTMAP正在运行	中危	1	RPC类	CVE-1999-0632	192.168.10.55
15	远程SSH服务器允许的客户端的SSH协议可列表	中危	1	信息收集类	--	192.168.10.55

## 环境描述:

服务器: CentOS 6.5 (Final)

服务器 IP: 192.168.10.55

客户机: Windows 10 -1908

客户机 IP: 192.168.10.94

## 操作步骤:

- 1、检查操作系统上的组件版本, 确认存在隐患

```
[root@localhost ~]# openssl version  
  
OpenSSL 1.0.1e-fips 11 Feb 2013  
  
[root@localhost ~]# ssh -V  
  
OpenSSH_5.3p1, OpenSSL 1.0.1e-fips 11 Feb 2013
```

- 确保 selinux 关闭

```
setenforce 0  
  
sed -i 's/enforcing/disabled/g' /etc/selinux/config
```

- 2、根据自身系统评估, 下载稳定版本的组件源码包, 下载地址:

<https://www.openssl.org/>

<https://www.openssh.com/>

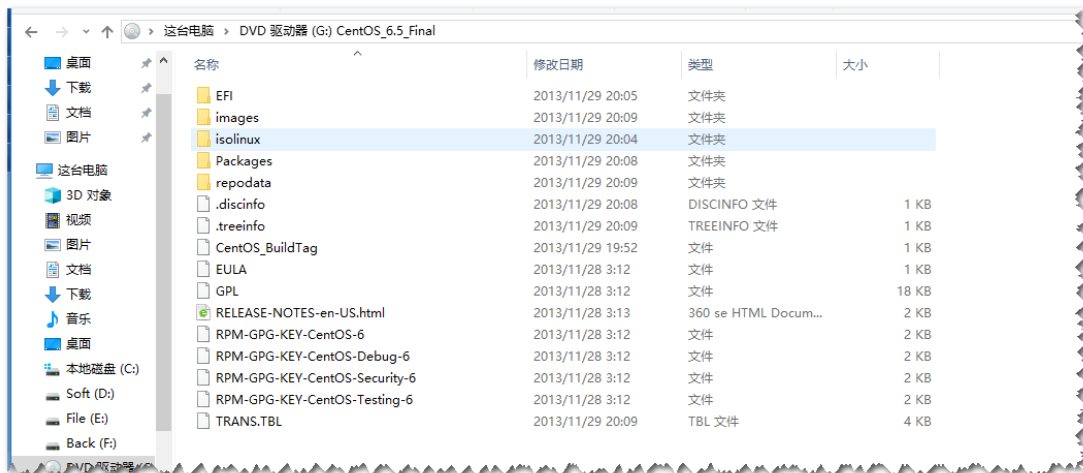
本次使用的版本为: OpenSSH\_8.0p1, OpenSSL 1.0.2s 28 May 2019

- 3、备份原有 YUM 源

```
[root@localhost ~]# tar -xvf /etc/yum.repos.d/Centos*
```

```
[root@localhost ~]# rm -rf /etc/yum.repos.d/Centos*
```

#### 4、将镜像挂载，部署于 FTP 的 anonymous 用户下（部署过程略）



#### 5、清除原有 yum 源，部署自身新 yum 源

```
yum clean all &> /dev/null  
  
touch /etc/yum.repos.d/vcentos.repo  
  
cat >> /etc/yum.repos.d/vcentos.repo <<EOF  
  
[venus_yum]  
  
gpgcheck = 0  
  
enabled = 1  
  
baseurl = ftp://192.168.10.94  
  
name = this is my yum  
  
EOF
```

- 检查 yum 源是否正确建立？

```
[root@localhost ~]# cat /etc/yum.repos.d/vcentos.repo  
  
[rhel7]
```

```
name = this is my yum

enabled = 1

pgpcheck = 0

baseurl =ftp://192.168.10.94/
```

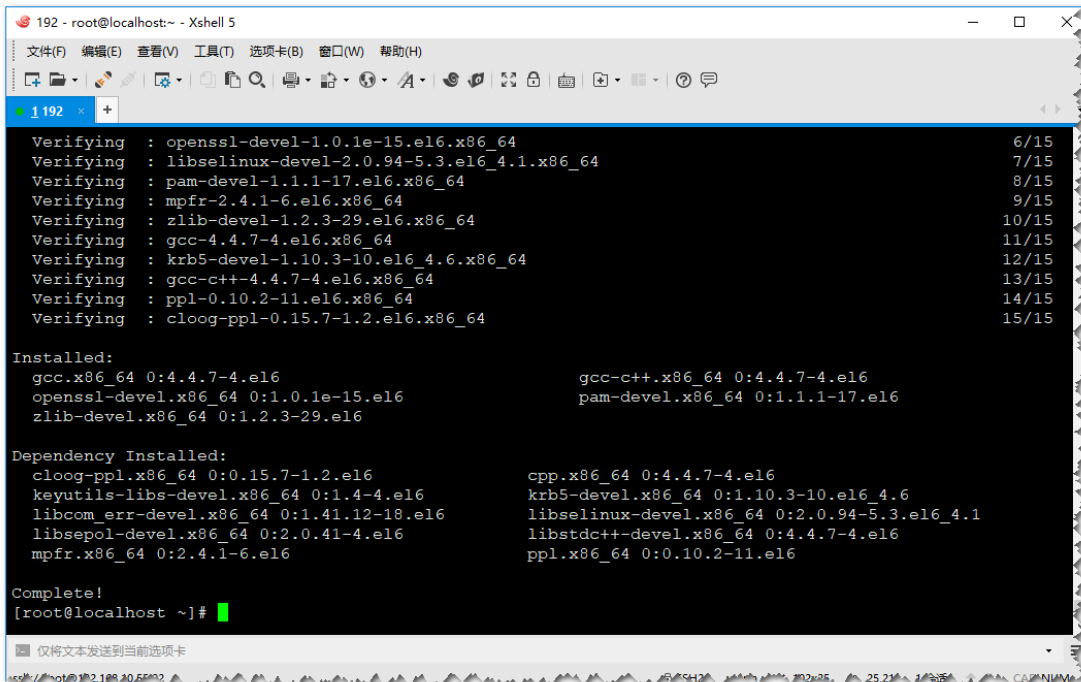
- yum makecache 确认 yum 源正常使用。

```
[root@localhost ~]# yum makecache
Loaded plugins: fastestmirror, refresh-packagekit, security
Loading mirror speeds from cached hostfile
rhel7 | 4.0 kB 00:00
Metadata Cache Created
```

## 6、安装相应编译依赖组件

```
yum install -y gcc gcc-c++ zlib zlib-devel pam-devel openssl-devel perl
```

出现下列提示则成功！



```
Verifying : openssl-devel-1.0.1e-15.el6.x86_64 6/15
Verifying : libselinux-devel-2.0.94-5.3.el6_4.1.x86_64 7/15
Verifying : pam-devel-1.1.1-17.el6.x86_64 8/15
Verifying : mpfr-2.4.1-6.el6.x86_64 9/15
Verifying : zlib-devel-1.2.3-29.el6.x86_64 10/15
Verifying : gcc-4.4.7-4.el6.x86_64 11/15
Verifying : krb5-devel-1.10.3-10.el6_4.6.x86_64 12/15
Verifying : gcc-c++-4.4.7-4.el6.x86_64 13/15
Verifying : ppl-0.10.2-11.el6.x86_64 14/15
Verifying : cloog-ppl-0.15.7-1.2.el6.x86_64 15/15

Installed:
gcc.x86_64 0:4.4.7-4.el6 gcc-c++.x86_64 0:4.4.7-4.el6
openssl-devel.x86_64 0:1.0.1e-15.el6 pam-devel.x86_64 0:1.1.1-17.el6
zlib-devel.x86_64 0:1.2.3-29.el6

Dependency Installed:
cloog-ppl.x86_64 0:0.15.7-1.2.el6 cpp.x86_64 0:4.4.7-4.el6
keyutils-libs-devel.x86_64 0:1.4-4.el6 krb5-devel.x86_64 0:1.10.3-10.el6_4.6
libcom_err-devel.x86_64 0:1.41.12-18.el6 libselinux-devel.x86_64 0:2.0.94-5.3.el6_4.1
libsepol-devel.x86_64 0:2.0.41-4.el6 libstdc++-devel.x86_64 0:4.4.7-4.el6
mpfr.x86_64 0:2.4.1-6.el6 ppl.x86_64 0:0.10.2-11.el6

Complete!
[root@localhost ~]#
```

7、通过多种方式上传组件源码到相关文件夹，升级后建议保留源码包，以便后期卸载和更新。

```
wget http://192.168.10.94/openssh-8.0p1.tar.gz
```

wget http://192.168.10.94/openssl-1.0.2s.tar.gz

```
[root@localhost ~]# wget http://192.168.10.94/openssh-8.0p1.tar.gz
--2019-06-16 07:41:54-- http://192.168.10.94/openssh-8.0p1.tar.gz
正在连接 192.168.10.94:80... 已连接。
已发出 HTTP 请求，正在等待回应... 200 OK
长度: 1597697 (1.5M) [application/octet-stream]
正在保存至: "openssh-8.0p1.tar.gz"

100%[=====>] 1,597,697  --.-K/s  in 0.1s
2019-06-16 07:41:54 (15.4 MB/s) - 已保存 "openssh-8.0p1.tar.gz" [1597697/1597697]

[root@localhost ~]# wget http://192.168.10.94/openssl-1.0.2s.tar.gz
--2019-06-16 07:41:57-- http://192.168.10.94/openssl-1.0.2s.tar.gz
正在连接 192.168.10.94:80... 已连接。
已发出 HTTP 请求，正在等待回应... 200 OK
长度: 5349149 (5.1M) [application/octet-stream]
正在保存至: "openssl-1.0.2s.tar.gz"

100%[=====>] 5,349,149  15.4M/s  in 0.3s
2019-06-16 07:41:57 (15.4 MB/s) - 已保存 "openssl-1.0.2s.tar.gz" [5349149/5349149]
```

## 7、开始编译安装 OpenSSL 组件

```
tar -xvf openssl-1.0.2s.tar.gz

cd openssl-1.0.2s

./config --prefix=/usr --openssldir=/etc/ssl --shared zlib

make &&make install

ldconfig
```

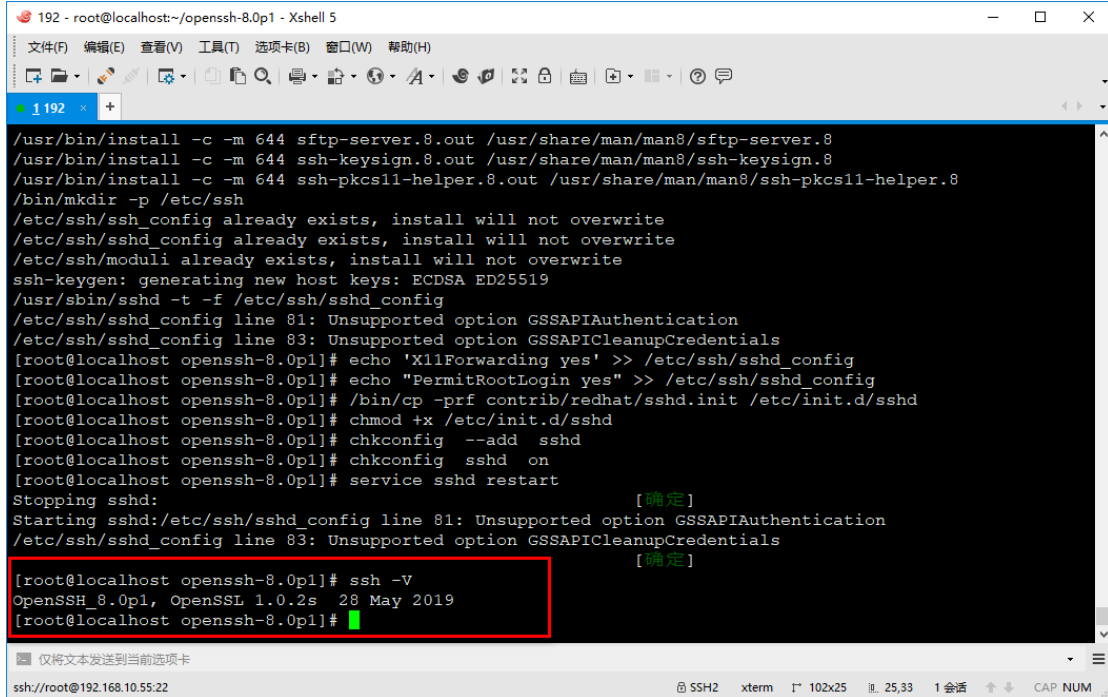
## 8、编译成功后，再继续安装 OpenSSH 组件。

```
192 - root@localhost:~/openssl-1.0.2s - Xshell 5
文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)
1 192
make[1]: Nothing to be done for `install'.
make[1]: Leaving directory `/root/openssl-1.0.2s/test'
making install in tools...
make[1]: Entering directory `/root/openssl-1.0.2s/tools'
make[1]: Leaving directory `/root/openssl-1.0.2s/tools'
installing libcrypto.a
installing libssl.a
installing libcrypto.so.1.0.0
installing libssl.so.1.0.0
make[1]: Entering directory `/usr/lib64'
make[2]: Entering directory `/usr/lib64'
make[2]: Leaving directory `/usr/lib64'
make[2]: Entering directory `/usr/lib64'
make[2]: Leaving directory `/usr/lib64'
make[1]: Leaving directory `/usr/lib64'
cp libcrypto.pc /usr/lib64/pkgconfig
chmod 644 /usr/lib64/pkgconfig/libcrypto.pc
cp libssl.pc /usr/lib64/pkgconfig
chmod 644 /usr/lib64/pkgconfig/libssl.pc
cp openssl.pc /usr/lib64/pkgconfig
chmod 644 /usr/lib64/pkgconfig/openssl.pc
[root@localhost openssl-1.0.2s]# ldconfig
[root@localhost openssl-1.0.2s]# openssl version
OpenSSL 1.0.2s 28 May 2019
[root@localhost openssl-1.0.2s]#
```

## 9、编译安装 OpenSSH

```
tar -xvf openssl-8.0p1.tar.gz
cd openssl-8.0p1
./configure --prefix=/usr --sysconfdir=/etc/ssh --with-md5-
passwords --with-pam --with-zlib --with-openssl-includes=/usr --
with-privsep-path=/var/lib/ssh
make && make install
echo 'X11Forwarding yes' >> /etc/ssh/sshd_config
echo "PermitRootLogin yes" >> /etc/ssh/sshd_config
/bin/cp -prf contrib/redhat/sshd.init /etc/init.d/ssh
chmod +x /etc/init.d/ssh
sed -i 's/^GSSAPIAuthentication/#&/' /etc/ssh/sshd_config
chkconfig --add sshd
chkconfig sshd on
service sshd restart
```

## ssh -V



```
192 - root@localhost:~/openssh-8.0p1 - Xshell 5
文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)
1 192
/usr/bin/install -c -m 644 sftp-server.8.out /usr/share/man/man8/sftp-server.8
/usr/bin/install -c -m 644 ssh-keysign.8.out /usr/share/man/man8/ssh-keysign.8
/usr/bin/install -c -m 644 ssh-pkcs11-helper.8.out /usr/share/man/man8/ssh-pkcs11-helper.8
/bin/mkdir -p /etc/ssh
/etc/ssh/ssh_config already exists, install will not overwrite
/etc/ssh/sshd_config already exists, install will not overwrite
/etc/ssh/moduli already exists, install will not overwrite
ssh-keygen: generating new host keys: ECDSA ED25519
/usr/sbin/sshd -t -f /etc/ssh/sshd_config
/etc/ssh/sshd_config line 81: Unsupported option GSSAPIAuthentication
/etc/ssh/sshd_config line 83: Unsupported option GSSAPICleanupCredentials
[root@localhost openssh-8.0p1]# echo 'X11Forwarding yes' >> /etc/ssh/sshd_config
[root@localhost openssh-8.0p1]# echo "PermitRootLogin yes" >> /etc/ssh/sshd_config
[root@localhost openssh-8.0p1]# /bin/cp -prf contrib/redhat/sshd.init /etc/init.d/sshd
[root@localhost openssh-8.0p1]# chmod +x /etc/init.d/sshd
[root@localhost openssh-8.0p1]# chkconfig --add sshd
[root@localhost openssh-8.0p1]# chkconfig sshd on
[root@localhost openssh-8.0p1]# service sshd restart
Stopping sshd: [确定]
Starting sshd:/etc/ssh/sshd_config line 81: Unsupported option GSSAPIAuthentication
/etc/ssh/sshd_config line 83: Unsupported option GSSAPICleanupCredentials [确定]
[root@localhost openssh-8.0p1]# ssh -V
OpenSSH_8.0p1, OpenSSL 1.0.2s 28 May 2019
[root@localhost openssh-8.0p1]#
```

当出现 OpenSSH\_8.0p1, OpenSSL 1.0.2s 28 May 2019 时，相应组件完成更新！

注：以下报错已经在上述代码中注释处理，如服务器有对 GSSAPI 功能有需求，请自行调整。

```
Starting sshd:/etc/ssh/sshd_config line 81: Unsupported option  
GSSAPIAuthentication
```

```
/etc/ssh/sshd_config line 83: Unsupported option GSSAPICleanupCredentials
```

另外：根据等级保护测评要求，不允许 root 账户直接登录，在 OpenSSH 7.4 以后版本默认也不允许 root 直接登录服务器，上述代码允许 root 账户直接登录，如无需该功能，请删除该行代码

```
echo "PermitRootLogin yes" >> /etc/ssh/sshd_config
```

10、删除部分编译环境，确保系统最小化安装和安全

```
yum remove perl gcc openssl-devel zlib-devel -y
```

11、再次对服务器复查，该漏洞问题被修复！建议重启服务器确保相

关功能无误。

The screenshot displays the '天镜 脆弱性扫描与管理系统' (Cyberspection Vulnerability Assessment and Management System) interface. The main content area shows a '漏洞列表' (Vulnerability List) table with the following data:

序号	漏洞名称	危险级别	主机数量	漏洞类型	CVE编号	存在主机
1	ssh_检测类型和版本	低	1	守护进程类	--	192.168.10.55
2	ssh_协议版本	低	1	守护进程类	--	192.168.10.55
3	SSH信息获取	中	1	信息收集类	CVE-1999-0634	192.168.10.55
4	ICMP时间戳获取	中	1	信息收集类	CVE-1999-0524	192.168.10.55
5	RPCBIND/PORTMAP正在运行	中	1	RPC类	CVE-1999-0632	192.168.10.55
6	远程SSH服务器允许的客户端的SSH协议可列取	中	1	信息收集类	--	192.168.10.55

At the bottom of the table, it indicates '共6条数据' (Total 6 records).