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。

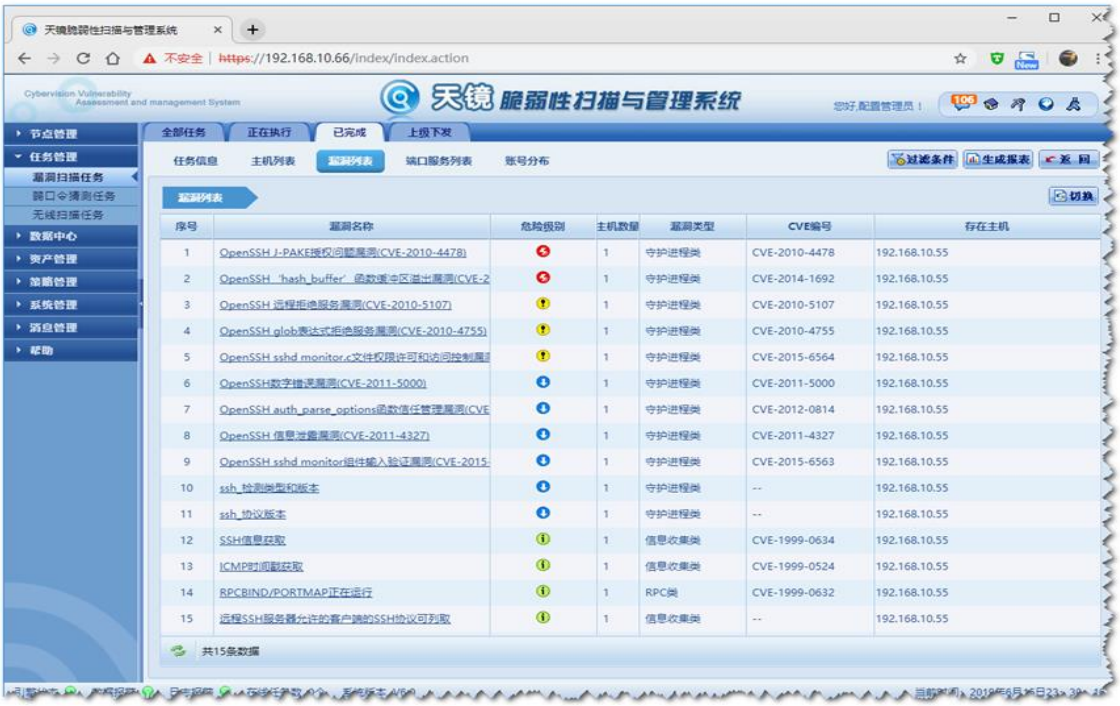
需自行准备：FTP、HTTP 服务器软件，相关系统 iso 镜像包。

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。



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/

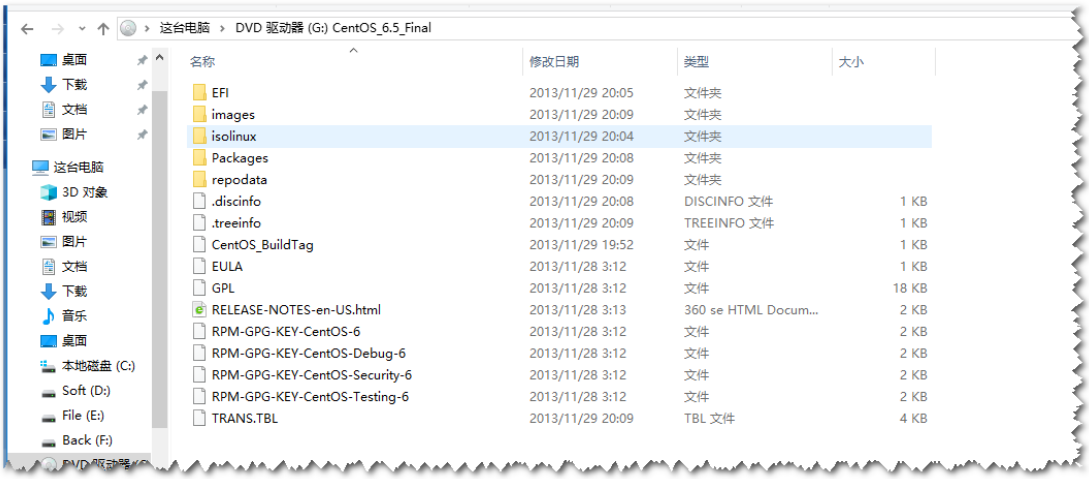
本次使用的版本为：OpenSSH_8.0p1, OpenSSL 1.0.2s 28 May 2019

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

gpgcheck = 0

baseurl =ftp://192.168.10.94/

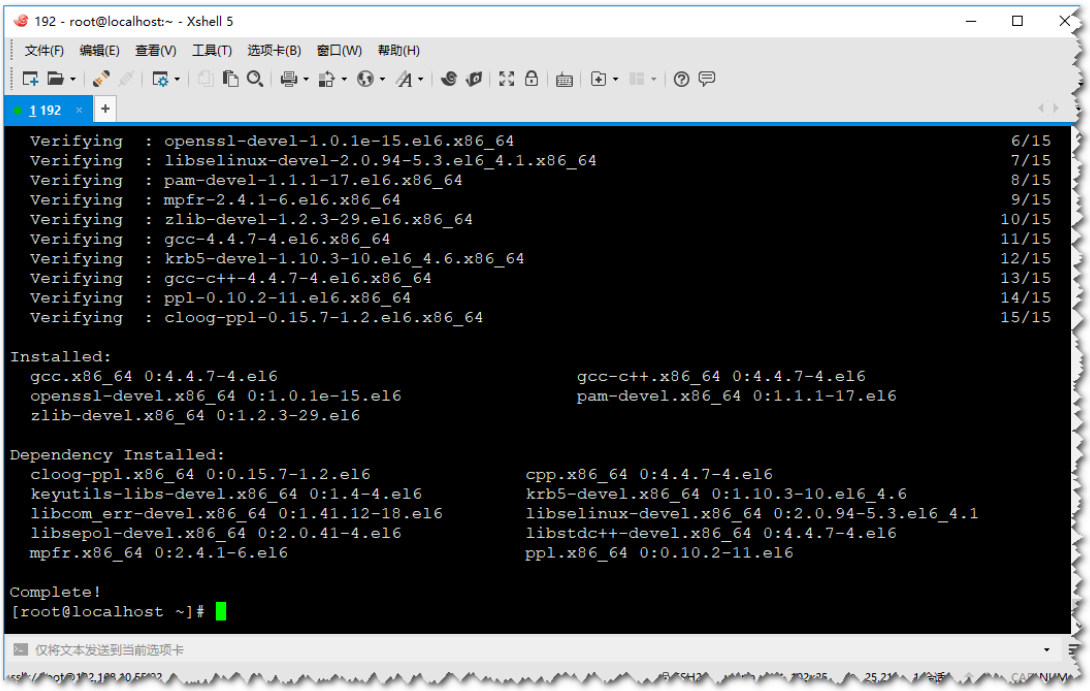
- yum makecache 确认 yum 源正常使用。

```
[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！



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。

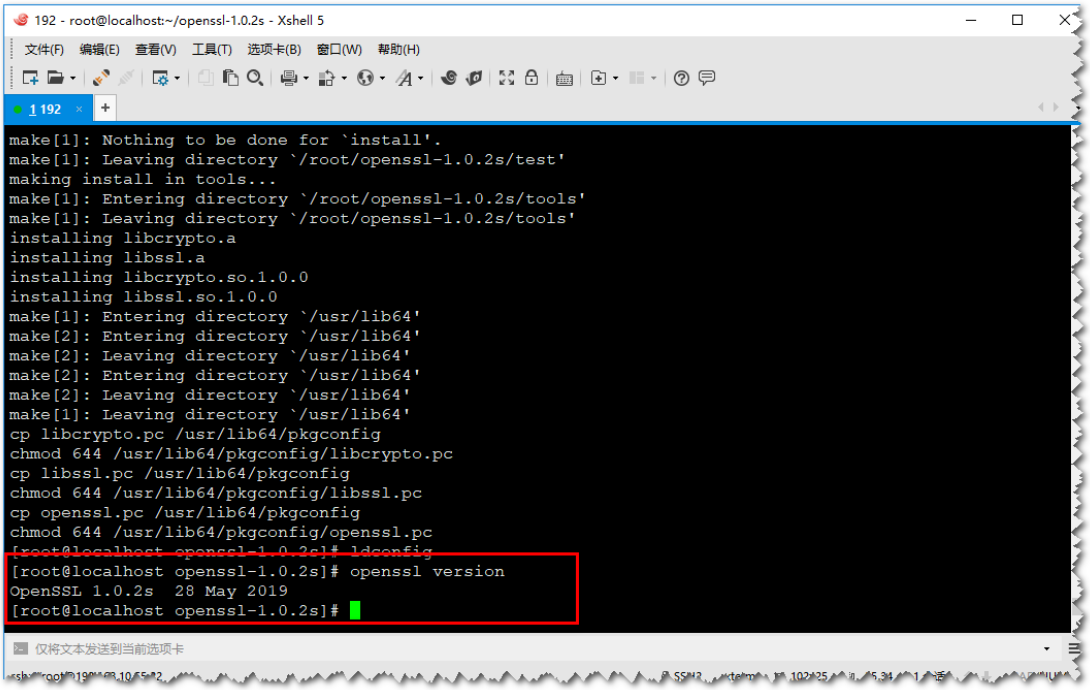
wget http://192.168.10.94/openssh-8.0p1.tar.gz

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

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
```

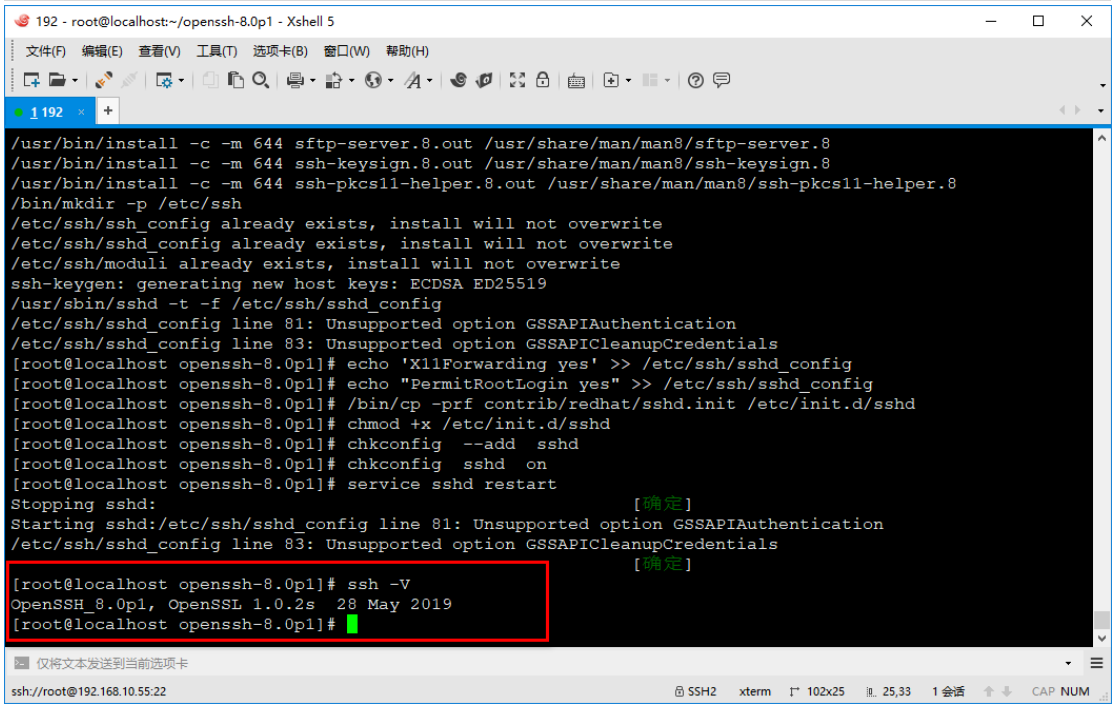
8、编译成功后，再继续安装 OpenSSH 组件。



9、编译安装 OpenSSH

```
tar -xvf openssh-8.0p1.tar.gz

cd openssh-8.0p1

./configure --prefix=/usr --sysconfdir=/etc/ssh --with-md5-passwords --with-pam --with-zlib --with-openssl-includes=/usr --with-privsep-path=/var/lib/sshd

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/sshd

chmod +x /etc/init.d/sshd

sed -i 's/^GSSAPIAuthentication/#&/' /etc/ssh/sshd_config

chkconfig --add sshd

chkconfig sshd on

service sshd restart
```

ssh -V



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。


天镜脆弱性扫描与管理系统
不安全 | https://192.168.10.66/index/index.action
Cybervision Vulnerability Assessment and management System
天镜 脆弱性扫描与管理系统
您好,配置管理员!
节点管理
任务管理
漏洞扫描任务
弱口令猜测任务
无线扫描任务
数据中心
资产管理
策略管理
系统管理
消息管理
帮助
全部任务
正在执行
已完成
上级下发
任务信息
主机列表
漏洞列表
端口服务列表
账号分布
过滤条件
生成报表
返 回
漏洞列表
切换
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 1 守护进程类 -- 192.168.10.55
2 ssh_协议版本 1 守护进程类 -- 192.168.10.55
3 SSH信息获取 1 信息收集类 CVE-1999-0634 192.168.10.55
4 ICMP时间戳获取 1 信息收集类 CVE-1999-0524 192.168.10.55
5 RPCBIND/PORTMAP正在运行 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 1 信息收集类 -- 192.168.10.55
共6条数据