**RHEL6.4下的openssh漏洞升级**

**2014-5-3**

今天给本地的移动公司处理了一起RHEL6.4openssh漏洞问题，移动公司使用专用的漏洞扫描工具发现了如下漏洞：

主要是因为openssh版本低，并且ssh设置不达标。必须升级系统自带的openssh版本到最新版本，并且适当修改ssh的配置文件，就可以修复类似的漏洞。

openssh的运转需要openssl和zlib的支持，升级openssh最好同步升级openssl和zlib，避免出现不匹配的现象。

**目前3个组件的最新版本是:**

* openssh-6.6p1.tar.gz

下载地址<http://www.oschina.net/news/49792/openssh-6-6>

* openssl-1.0.1g.tar.gz

下载地址<http://www.openssl.org/source/>

* zlib-1.2.8.tar.gz

下载地址<http://www.zlib.net/>

**系统自带的三个组件的版本分别是：**

* openssh-5.3

**ssh –V**是查看当前运行的openssh版本，注意是V是大写，linux严格遵循大小写



* openssl-1.0.0-27



* zlib-1.2.3-29



**升级步骤：**

1. 保证gcc已经正确安装，编译源码需要
2. 如果是远程升级，请打开系统的telnet服务，以避免在ssh升级过程中出错，无法使用ssh服务远程连接；如果是在机器旁边操作，这步可忽略。如何打开telnet服务请参考其他文档
3. 下载3个源码包
4. 使用winscp上传3个源码包到指定路径

/usr/local/src

1. 解压缩3个包
* tar zxvf openssh-6.6p1.tar.gz
* tar zxvf openssl-1.0.1g.tar.gz
* tar zxvf zlib-1.2.8.tar.gz



1. 编译安装zlib
* cd zlib-1.2.8
* ./configure –prefix=/usr/local/zlib
* make
* make install
1. 编译安装openssl
* cd openssl-1.0.1g
* **./config** –prefix=/usr/local/openssl

**(注意是config而不是configure)**

* make
* make install
1. 编译安装openssh
* cd openssh-6.6pl
* ./configure --prefix=/usr --sysconfdir=/etc/ssh --with-pam --with-zlib=/usr/local/zlib --with-ssl-dir=/usr/local/openssl --with-md5-passwords

（注意，如果 configure 时提示 PAM 有错误，那一般是因为系统中没有安装 pam-devel RPM 包，找到安装光盘，安装 pam-devel 就可以解决啦）

* make
* make install
1. 升级完成，查看升级完成后的openssh版本

ssh –V



已经成功升级为6.6的 版本。

**修改一些ssh配置**

1. 不允许使用ssh v1 协议，只允许使用sshv2协议

其实在RHEL6.4 版本中，默认就是这样设置的不需要改

1. 禁用X11转发

去掉x11Forwarding no前面的#

在x11Forwarding yes前加#

