**中国电信广东公司**

**SSH安全漏洞加固**

**（2015年6月）**

# 文档目的

为中国电信广东公司建立安全漏洞知识库，特制定本文档。

本文档是为了让大家对各种安全威胁的产生原因、常见攻击手段有更深入的了解，并且作为各种安全威胁的修补方案标准，以便大家能够快速的定位漏洞代码和解除安全隐患。最大程度降低安全缺陷，减少业务系统不稳定、隐藏通道、软件BUG等安全隐患。

# 漏洞描述

使用SOC平台对设备进行安全检查时，发现Solaris系统的主机存在漏洞，由于Solaris的SSH为定制版本，因此需要到Solaris官网下载SSH包进行升级解决。

# 升级环境

操作系统：Solaris 10

软件版本：Sun\_SSH\_1.1.4

# 升级SSH

升级前ssh版本：



升级步骤：

1. 检查设备是否有7za指令，有则直接跳到第3步，无则进入第2步；
2. 安装补丁包：



指令：

#unzip 137322-02.zip

#patchadd 137322-02

1. SSH（1.1.4版本）升级包：



开启telnet服务，至少开启两个root窗口。

#svcadmin enable telnet

如果使用telnet登录时提示：



解决方法：

注释掉 /etc/default/login文件中的CONSOLE=/dev/console

升级SSH

把ssh.tar 拷贝到系统中

#tar xf ssh.tar

#cd ssh

bash-3.2# ls

SUNWsshcu  SUNWsshdr  SUNWsshdu  SUNWsshr   SUNWsshu

#svcadm disable ssh

#pkgadd -d .

The following packages are available:

  1  SUNWsshcu     SSH Common, (Usr)

                   (i386) 11.10.0,REV=2005.01.21.16.34

  2  SUNWsshdr     SSH Server, (Root)

                   (i386) 11.10.0,REV=2005.01.21.16.34

  3  SUNWsshdu     SSH Server, (Usr)

                   (i386) 11.10.0,REV=2005.01.21.16.34

  4  SUNWsshr      SSH Client and utilities, (Root)

                   (i386) 11.10.0,REV=2005.01.21.16.34

  5  SUNWsshu      SSH Client and utilities, (Usr)

                   (i386) 11.10.0,REV=2005.01.21.16.34

Select package(s) you wish to process (or 'all' to process

all packages). (default: all) [?,??,q]: (直接回车，全选）

下面全部yes。

#svcadm enbale ssh

#svcs -a|grep ssh (确认是否已经启动）

#ssh -V看版本是否升级

升级后ssh版本：

