CERT Advisory CA-1995-15 SGI lp Vulnerability

Original issue date: November 8, 1995
Last revised: September 23, 1997
Updated Copyright statement

A complete revision history is at the end of this file.

The CERT Coordination Center has had several security incidents reported to us involving the lp account on the Silicon Graphics, Inc. (SGI) IRIX system. As distributed by SGI, the lp account, as well as other accounts, has no password on a newly installed system. The lp account, which is used by the *lp(1)* program for remote printing, and other accounts are initially configured without passwords to provide easy "plug-and-play" install and operation. However, these password-less accounts are well known by intruders and allow unintended access to your system.

In the documentation that SGI distributes with their systems, these password-less accounts are specifically addressed in the "IRIX Advanced Site and Server Administrative Guide" in the chapter on System Security. The documentation recommends disabling the login for the lp account. It also recommends that you create passwords for the following accounts immediately: demos, guest, lp, nuucp, root, tour, tutor, and 4Dgifts. The documentation includes guidelines for choosing good passwords.

To determine if your system is vulnerable, use the following command as root to display the status of all password-less accounts:

```
# /bin/passwd -sa | /bin/awk '$2 == "NP" {print $0}'
```

If this command displays any accounts, especially the lp account, then your system is vulnerable. To address this vulnerability, we recommend using the workarounds in Section III below.

We will update this advisory as we receive additional information. Please check advisory files regularly for updates that relate to your site.

I. Description

The SGI IRIX system as distributed has some accounts without passwords. Among the accounts that are password-less is the lp account. This account is used in part by the *lp(1)* program to manage object and spooled data files in the /var/spool/lp directory (for IRIX 4.X, this directory is /usr/spool/lp). The account is created without a password because *lp(1)* uses *rsh(1)* to transfer files from print clients to print servers.

II. Impact

Remote users can gain access to systems without authentication. The level of privilege gained depends on the password-less account used to access a system.

Although the scope of this advisory is the lp account, keep in mind that any account without a password (or with an easy-to-guess password) is a point for access without authentication.

III. Solution

The general solution is to lock all accounts that do not have passwords. Section A below describes how to do that.

Section B suggests one way to re-enable print client to print server communication.

A. Lock each password-less account.

Store the following script in /tmp/CheckPasswords for example and then run it as root on your machine to lock each password-less account. The password installed will not allow the accounts to be used as login accounts. See the *passwd(1)* manual page for more details. Note that this script only locks accounts on the local machine. If there are password-less accounts in NIS, those accounts will not be locked by this script.

```
-----------------------cut here--8<-----------------------
#!/bin/sh
for account in `/bin/passwd -sa | /bin/awk '$2 == "NP" {print $1}'`
do
        /bin/echo Locked the $account account
        /bin/passwd -l $account
done
-----------------------cut here--8<-----------------------
```

The first time the script is run, it should display something similar to the following:

```
        # sh /tmp/CheckPasswords
        Locked the tutor account
        Locked the tour account
        Locked the lp account
        ...
```

If the script locked an account, run the script again. This time it should produce no output because all password-less accounts have now been locked.

B. Re-enable print client to print server communication.

(We have verified with SGI that you can use the script in this section to re-enable the print client to print server communication. SGI has asked us to make it clear, however, that they do not have the resources to handle issues relating to the use of wrappers.)

Note that, in general, the CERT Coordination Center recommends that the rlogin and rsh services be blocked at your Internet routers and turned off on all of your machines. If you have turned the rsh service off on your print server, you will need to turn it back on on that machine. If you decide to do this, we strongly recommend that you install and use a TCP/IP wrapper program to restrict the set of machines that can connect to your print server's rsh service. A TCP/IP wrapper program is available from

ftp://ftp.cert.org/pub/tools/tcp_wrappers/tcp_wrappers_7.2.tar.Z
MD5 (tcp_wrappers_7.2.tar.Z) = 883d00cbd2dedd9bfc783b7065740e74

Once the rsh service is turned on on your print server and a TCP/IP wrapper program installed and configured, you then need to define the set of machines that can communicate with your print server.

For each IRIX system that controls a printer, the lp account needs to be changed to re-enable print client to print server communication. To do this, the lp account on each print server needs a .rhosts file in lp's home directory, typically /var/spool/lp (for IRIX 4.X, this directory is /usr/spool/lp). The owner and group of this file must be the same as that of the lp account. Its contents are lines of the form:

```
        print_client_name       lp
```

Each line identifies the name of the print client and indicates that the lp account is the account that is allowed to rsh from the print client to the print server.

The following shows an example of configuring communication from a print client (named "client") to a print server. This configuration need only be done on a print server. The ping command is used to determine the print client's formal name according to whatever host resolution scheme is in place. That name is stored in the .rhosts file. The last two lines, the ping and the echo, need to be repeated for each client of a print server.

```
# /bin/awk -F: '$1 == "lp" {print $0}' /etc/passwd
lp:*LK*:9:9:Print Spooler Owner:/var/spool/lp:/bin/sh
# cd `/bin/awk -F: '$1 == "lp" {print $6}' /etc/passwd`
# /bin/touch .rhosts
# /bin/chown lp .rhosts
# /bin/chgrp lp .rhosts
# /bin/chmod 600 .rhosts
# /usr/etc/ping -c 1 client | /bin/awk '$1 == "PING" {print $2}'
client.YourDomain
# /bin/echo client.YourDomain lp >> .rhosts
```

The CERT Coordination Center staff thanks Silicon Graphics Inc. and Christopher Kranz of Princeton University for their support in responding to this problem.

UPDATES

Silicon Graphics, Inc. have issued a Security Advisory concerning this vulnerability (19951002-01-I). Their advisory can be obtained from

ftp://sgigate.sgi.com/security

We have received additional information from one member of our constituency regarding the vulnerability in the SGI printing system and the accounts without passwords. The supercomputer NEC SX-3 running "SUPER-UX unix 5.10 1 SX-3" (which is very similar to IRIX) also has the same vulnerability.

(As far as we are aware there are only about 30 machines [in the world] running this OS.)

Revision History

```
Sep. 23, 1997  Updated copyright statement
Aug. 30, 1996  Information previously in the README was inserted
               into the advisory.
Dec. 20, 1995  Updates section - Added a pointer to SGI advisory and a note
               about the supercomputer NEC SX-3.
```