CERT Advisory CA-1995-09 Solaris ps Vulnerability

Original issue date: August 29, 1995
Last revised: September 23, 1997
Updated Copyright statement

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

The text of this advisory is taken primarily from AUSCERT advisory AA-95.07, with their permission.

A vulnerability exists in Solaris systems that allows a race condition to be exploited to gain root access. The essential problem is that the *ps(1)* program maintains a data file in the /tmp directory, and the /tmp directory is world-writable, allowing users to delete other users' files in /tmp. This vulnerability affects Solaris 2.x (SunOS 5.x) systems.

An exploit program for this vulnerability has been published. We urge you to take the actions described in Section III as soon as possible.

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

I. Description

A race condition exists in at least one Solaris 2.x (SunOS 5.x) system program that can be exploited to gain root access if the user has access to the temporary files. Access to temporary files may be obtained if the permissions on the /tmp and /var/tmp directories are set incorrectly. The permissions on the /tmp directory are often reset incorrectly by the system if tmpfs (which is mounting swap as /tmp) is in use.

II. Impact

Users logged in to the system may gain unauthorized root privileges.

III. Solution

A. Determine if your system is vulnerable

To determine if you are running tmpfs, the following command can be used to verify if the file system for /tmp is swap:

```
% /usr/sbin/df -k /tmp
Filesystem          kbytes    used   avail capacity  Mounted on
swap                 28348     12    28336     0%    /tmp
```

or look in the file /etc/vfstab for the configuration line:

```
#device     device   mount    FS      fsck    mount     mount
#to mount   to fsck  point    type    pass    at boot   options
swap          -      /tmp     tmpfs     -      yes         -
```

If either of these two conditions exist, then you are running tmpfs and the system may automatically reset the permission bits of /tmp at the next reboot.

To verify if your configuration is currently vulnerable, the following command may be used:

```
% /usr/bin/ls -ld /tmp
drwxrwxrwt   2 root     root       61 Aug 15 12:12 /tmp
```

If the sticky bit (t) is not set (it will be an x), then the system is vulnerable. In addition, we recommend that the owner and group for /tmp be changed to root and root, respectively.

B. Perform the following workarounds

These workarounds have been verified with Sun Microsystems. Apply these workarounds until you an install a patch. (Patch information is in Sec. C. below.)

1. Immediate - fix /tmp permissions

A workaround that takes effect immediately is to set the sticky bit on the /tmp directory using the following command as root:

```
# /usr/bin/chmod 1777 /tmp
```

Note that this command must be performed after each reboot if you are mounting swap as /tmp (using tmpfs).

In addition, the ownership and group membership of the /tmp directory should be verified using /usr/bin/ls -ld /tmp, and if incorrect may be reset by:

```
# /usr/bin/chown root /tmp
# /usr/bin/chgrp root /tmp
```

The AUSCERT UNIX Security Checklist addresses this issue in Section 5.5. This section is reproduced in the appendix of this advisory. The entire AUSCERT checklist may be obtained from these locations.

Sites outside of Australia should use the ftp.cert.org FTP site.

ftp://ftp.cert.org/pub/tech_tips/AUSCERT_checklist_1.1
ftp://ftp.auscert.org.au/pub/auscert/papers/unix_security_checklist_1.1

2. Permanent - make the above change to /tmp permissions permanent

The change noted in item B.1 above will be lost upon reboot. To make the changes permanent, create the following script as /etc/init.d/tmpfsfix:

```
-----------------------------cut here--8<----------------------------
#!/bin/sh

if [ -d /tmp ]
then
   /usr/bin/chmod 1777 /tmp
   /usr/bin/chgrp root /tmp
   /usr/bin/chown root /tmp
fi
------------------------------cut here---8<--------------------------
```

After creating this file, the following commands should be issued as root to make the file executable, set appropriate owner and group, and create the necessary symbolic link to ensure that it is executed upon reboot appropriately:

```
             # /usr/bin/ln -s /etc/init.d/tmpfsfix /etc/rc2.d/S06tmpfix
             # /usr/bin/chmod 744  /etc/init.d/tmpfsfix
             # /usr/bin/chown root /etc/init.d/tmpfsfix
             # /usr/bin/chgrp sys /etc/init.d/tmpfsfix
             # /bin/rm -f /etc/rc3.d/S79tmpfix
```

If you have done item B.1 above, you can reboot at your leisure. Otherwise, reboot your system now. In either case, verify the permissions of /tmp immediately after your next system reboot.

3. Check /var/tmp permissions

We recommend that you also check and correct the /var/tmp directory. Note that this directory is not usually mounted as tmpfs, so it normally would not be subject to automatic resetting of its permission bits on reboot.

```
% /usr/bin/ls -ld /var/tmp
drwxrwxrwt   2 root     root      512 Aug 15 11:35 /var/tmp
```

C. Install a vendor patch

On September 20, 1995, Sun Microsystems, Inc., provided the following information in their advisory.

Begin Text provided by vendor

II. Announcement of patches for Solaris 2.x "ps_data" vulnerability

A. Patch list

We have produced patches for the versions of SunOS shown below.

OS version	Patch ID	Patch File Name
5.3	101545-02	101545-02.tar.Z
5.4	102711-01	102711-01.tar.Z
5.4_x86	102712-01	102712-01.tar.Z

B. Patch notes

1. SunOS 4.1.x systems are not affected by this bug. 2. The fix has been applied to the upcoming version of Solaris.

III. Checksum Table

In the checksum table we show the BSD and SVR4 checksums and MD5 digital signatures for the compressed tar archives.

```
   File            BSD          SVR4        MD5
   Name            Checksum     Checksum    Digital Signature
   --------------- -----------  ----------  --------------------------------
   101545-02.tar.Z 41218    77  47754  153  A8FB866780E7207D26CF16210BCFDC83
   102711-01.tar.Z 17256    69  20376  138  98A449372C5ABBDB7C37B08BFE0E6ED7
   102712-01.tar.Z 29867    68  56717  136  E324004BB8C09990B2790CB5D29D3AF5
```

The checksums shown above are from the BSD-based checksum (on 4.1.x, /bin/sum; on Solaris 2.x, /usr/ucb/sum) and from the SVR4 version on Solaris 2.x (/usr/bin/sum).

End Text provided by vendor

Appendix: Excerpt from AUSCERT UNIX Security Checklist (Version 1.1) 5.5 File Permissions

- ENSURE that the permissions of /etc/utmp are set to 644.
- ENSURE that the permissions of /etc/sm and /etc/sm.bak are set to 2755.
- ENSURE that the permissions of /etc/state are set to 644.
- ENSURE that the permissions of /etc/motd and /etc/mtab are set to 644.
- ENSURE that the permissions of /etc/syslog.pid are set to 644.
  [**NOTE:** this may be reset each time you restart syslog.]
- DO consider removing read access to files that users do not need to access.
- ENSURE that the kernel (e.g., /vmunix) is owned by root, has group set to 0 (wheel on SunOS) and permissions set to 644.
- ENSURE that /etc, /usr/etc, /bin, /usr/bin, /sbin, /usr/sbin, /tmp and /var/tmp are owned by root and that the sticky-bit is set on /tmp and on /var /tmp (see G.14). Refer to the AUSCERT Advisory AA-95:05 (see A.1).
- ENSURE that there are no unexpected world writable files or directories on your system.
  See G.15 for example commands to find group and world writable files and directories.
- CHECK that files which have the SUID or SGID bit enabled, should have it enabled (see G.16).
- ENSURE the umask value for each user is set to something sensible like 027 or 077. (Refer to section E.1 for a shell script to check this).
- ENSURE all files in /dev are special files.

  Special files are identified with a letter in the first position of the permissions bits. See G.17 for a command to find files in /dev which are not special files or directories.

  Note: Some systems have directories and a shell script in /dev which may be legitimate. Please check the manual pages for more information.
- ENSURE that there are no unexpected special files outside /dev. See G.18 for a command to find any block special or character special files.

The CERT Coordination Center staff thanks AUSCERT, the Australian response team, for their permission to reuse text from their advisory AA-95.07 and for their cooperation and assistance.

UPDATES

If anyone has trouble retrieving the electronic file CA-95.09.Solaris.ps.vul, they should use the file name CA-95.09.Solaris-ps.vul.

Revision History

```
Sep. 23, 1997  Updated copyright statement
Aug. 30, 1996  Information previously in the README was inserted
                into the advisory. Updated version number of AUSCERT checklist
                and the appendix.
Sep. 20, 1995  Sec. III.A.1 - corrected the command and explanation for
                checking your configuration.
               Sec. III.B.1 - corrected commands for verifying ownership and
                group membership.
               Sec. III.B.2 - replaced this section, which was incorrect.
               Sec. III.B.3 - replaced the text and command.
               Sec. III.C - added this section, which contains Sun patch
                information.
               Appendix - corrected item 10.
               Updates section - added a note about the file name.
```