CERT Advisory CA-1994-06 Writable /etc/utmp Vulnerability

Original issue date: March 21, 1994
Last revised: September 19, 1997
updated copyright statement

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

The CERT Coordination Center has received information concerning a vulnerability that exists on systems where the file /etc/utmp is writable by any user on the system.

This vulnerability is being actively exploited; please review CA-94.01 Ongoing Network Monitoring Attacks.

The problem is known to affect Sun Microsystems, Inc. SunOS 4.1.X and Solaris 1.1.1 operating systems. Solbourne Computer, Inc. and other Sparc products using SunOS 4.1.X or Solaris 1.1.1 are also affected. Solaris 2.x and SunOS 4.1.3_U1 (Solaris 1.1.1) are not affected by this problem.

Patches can be obtained from Sun Answer Centers worldwide. They are also available via anonymous FTP from ftp.uu.net in the /systems/sun/sun-dist directory, and in Europe from ftp.eu.net in the /sun/fixes directory.

We queried several vendors in addition to Sun. The following vendors reported that their operating systems, as distributed by the vendor, are not affected by this problem:

Convex Computer Corporation
Digital Equipment Corporation
Data General Corporation
Hewlett-Packard Company IBM
Intergraph
Motorola, Inc.
NeXT, Inc.
Pyramid Technology Corporation
Sequent Computer Systems
Sony Corporation

Currently, we are not aware of /etc/utmp being writable on other systems. If your operating system is not explicitly mentioned above, and if you determine that /etc/utmp is writable by someone other than root, we encourage you to contact your vendor.

If /etc/utmp on your system is writable only by the root account, you need not be concerned about the vulnerability.

We recommend that sites check their /etc/utmp file to be sure it is not writable by users other than root. If it is generally writable, you should obtain patches from the system vendor or protect /etc/utmp as described below.

I. Description

If the file /etc/utmp is writable by users other than root, programs that trust the information stored in that file can be subverted.

II. Impact

This vulnerability allows anyone with access to a user account to gain root access.

III. Solution

The solutions to this vulnerability are to either (a) protect the file, or (b) patch all the programs that trust it.

Note that SunOS 4.1.3_U1 (Solaris 1.1.1) is _not_ vulnerable to this problem.

A. To protect the file, make /etc/utmp writable only by root:

```
# chown root /etc/utmp

# chmod 644 /etc/utmp
```

B. Patches from Sun Microsystems

```
Program     Patch ID    Patch File Name
-------     ---------   ---------------
in.comsat   100272-07   100272-07.tar.Z
dump        100593-03   100593-03.tar.Z
syslogd     100909-02   100909-02.tar.Z
in.talkd    101480-01   101480-01.tar.Z
shutdown    101481-01   101481-01.tar.Z
write       101482-01   101482-01.tar.Z
```

```
Program     BSD          SVR4         MD5 Digital Signature
            Checksum     Checksum
-------     ---------    ---------    --------------------------------
in.comsat   26553  39    64651  78    912ff4a0cc8d16a10eecbd7be102d45c
dump        52095 242    41650 484    cdba530226e8735fae2bd9bcbfa47dd0
syslogd     61539 108    38239 216    b5f70772384a3e58678c9c1f52d81190
in.talkd    47917  44    32598  88    5c3dfd6f90f739100cfa4aa4c97f01df
shutdown    46562  80    56079 159    bfc257ec795d05646ffa733d1c03855b
write       61148  41    48636  81    f93276529aa9fc25b35679ebf00b2d6f
```

C. Clarifications added April 1, 1994

1. If you make /etc/utmp writable only by root, this should only affect programs that allocate pseudo terminal interfaces and want to add an appropriate entry to the /etc/utmp file. Such programs include *script(1)*, *cmdtool(1)*, *gfxtool(1)*, *shelltool(1)*, and *tektool(1)*. These programs will no longer be able to add an entry to /etc/utmp which means that programs such as *who(1)*, *syslogd(1)*, and others that use /etc/utmp will not know that an account is using that pseudo tty.
2. No program should be made setuid root just to workaround this problem. Setuid programs must be written very carefully to avoid creating yet more vulnerabilities.
3. The installation instructions on the syslogd patch do not point out that, until you stop and restart syslogd (or reboot the system), the old version is still running and the security hole has not been closed.

Revision History

```
Sep. 19,1997   Updated copyright statement
Aug. 30, 1996  Information previously in the README was inserted
               into the advisory.
Apr. 01, 1994  Intro. and Sec. III - added note that SunOS 4.1.3_U1 is not
               vulnerable.
Apr. 01, 1994  Sec. III.C - added this new section, which contains
               clarifications.
```