CERT Advisory CA-1991-19 AIX TFTP Daemon Vulnerability

Original issue date: October 17, 1991
Last revised: September 18, 1997
Attached copyright statement

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

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received information concerning a vulnerability in the TFTP daemon in all versions of AIX for IBM RS/6000 machines.

IBM is aware of this problem and a fix is available as apar number "ix22628". This patch is available for all AIX releases from "GOLD" to the current release.

NOTE: THIS IS AN UPDATED PATCH FROM ONE RECENTLY MADE AVAILABLE and fixes a security hole in the original patch. The SCCS id of the correct patch is tftpd.c 1.13.1.3 (*not* 1.13.1.2 or earlier versions). This can be checked using the following "what" command.

```
% what /etc/tftpd
/etc/tftpd:
56      1.13.1.3  tftpd.c, tcpip, tcpip312 10/10/91 09:01:48
tftpsubs.c      1.2  com/sockcmd/tftpd,3.1.2,9048312 10/8/89 17:40:55
```

IBM customers may call IBM Support (800-237-5511) and ask that the fix be shipped to them. The fix will appear in the upcoming 2009 update and the next release of AIX.

I. Description

Previous versions of tftpd did not provide a method for restricting TFTP access.

II. Impact

If TFTP is enabled at your site, anyone on the Internet can retrieve copies of your site's world-readable files, such as /etc/passwd.

III. Solution

A. Sites that do not need to allow tftp access should disable it.

This can be done by editing /etc/inetd.conf and deleting or commenting out the tftpd line:

```
#tftp     dgram     udp    wait    nobody  /etc/tftpd     tftpd -n
```

and then, as root, restarting inetd with the "refresh" command.

```
# refresh -s inetd
```

For more details on starting/stopping tftp, refer to documentation for the System Resource Controller (SRC) or the System Management Interface Tool (SMIT).

B. Sites that must run tftpd (for example, to support X terminals) should obtain and install the above patch AND create a /etc/tftpaccess.ctl file to restrict the files that are accessible.

The /etc/tftpaccess.ctl file should be writable only by root. Although the new /etc/tftpaccess.ctl mechanism provides a very general capability, the CERT/CC strongly recommends that sites keep this control file simple. For example, the following tftpaccess.ctl file is all that is necessary to support IBM X terminals:

```
# /etc/tftpaccess.ctl
# By default, all files are restricted if /etc/tftpaccess.ctl exists.
# Allow access to X terminal files.
  allow:/usr/lpp/x_st_mgr/bin
```

NOTE: Be CERTAIN to create the /etc/tftpaccess.ctl file.
If it does not exist then all world-readable files are accessible as in the current version of tftpd.

Installation Instructions:

1. Create an appropriate /etc/tftpaccess.ctl file.

1. From the directory containing the new tftpd module, issue the following commands as root.

```
# chmod 644 /etc/tftpaccess.ctl
# chown root.system /etc/tftpaccess.ctl
# mv /etc/tftpd /etc/tftpd.old
# cp tftpd /etc
# chmod 755 /etc/tftpd
# chown root.system /etc/tftpd
# refresh -s inetd
```

The CERT/CC wishes to thank Karl Swartz of the Stanford Linear Accelerator Center for bringing this vulnerability to our attention.

Revision History

```
September 18,1997  Attached Copyright Statement
```