CERT Advisory CA-1991-18 Active Internet tftp Attacks

Original issue date: September 27, 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) would like to alert you to automated tftp probes that have been occurring over the last few days. These probes have attacked Internet sites throughout the world and in most cases the file retrieved was /etc/passwd. However, other files such as /etc/rc may have been retrieved.

The CERT/CC is working with the site(s) that were used by intruders to launch the attacks. We are actively contacting those sites where we believe the retrievals were successful. We are urging all sites to carefully check their system configurations concerning tftp usage.

I. Description

Unrestricted tftp access allows remote sites to retrieve a copy of any world-readable file.

II. Impact

Anyone on the Internet can use tftp to retrieve copies of a site's sensitive files. For example, the recent incident involved retrieving /etc/passwd. The intruder can later crack the password file and use the information to login to the accounts. This method may provide access to the root account.

III. Solution

A. Sites that do not need tftp should disable it immediately by editing the system configuration file to comment out, or remove, the line for tftpd.

This file may be /etc/inetd.conf, /etc/servers, or another file depending on your operating system. To cause the change to be effective, it will be necessary to restart inetd or force inetd to read the updated configuration file.

B. Sites that must use tftp (for example, for booting diskless

clients) should configure it such that the home directory is changed. Example lines from /etc/inetd.conf might look like:

```
ULTRIX 4.0
tftp   dgram  udp  nowait  /etc/tftpd  tftpd -r /tftpboot

SunOS 4.1
tftp   dgram  udp  wait  root  /usr/etc/in.tftpd in.tftpd -s /tftpboot
```

As in item A. above, inetd must be restarted or forced to read the updated configuration file to make the change effective.

C. If your system has had tftp configured as unrestricted, the CERT/CC urges you to consider taking one of the steps outlined above and change all the passwords on your system.

Revision History

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