Software Engineering Institute
Carnegie Mellon University

1988 CERT Advisories

CERT Division

http://www.sei.cmu.edu

REV-03.18.2016.0

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

This report was prepared for the

SEI Administrative Agent
AFLCMC/AZS
5 Eglin Street
Hanscom AFB, MA 01731-2100

DM17-0052

Table of Contents

1 CA-1988-01: ftpd Vulnerability

Original issue date: December 1988
Last revised: September 16, 1997
Attached copyright statement

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

** The sendmail portion of this advisory is superseded by CA-95.05. **

There have been several problems or attacks which have occurred in the past few weeks. In order to help secure your systems we have gathered the following suggestions:

1. Check that you are using version 5.59 of sendmail with the debug option DISABLED. To verify the version try the following commands. Use the telnet program to connect to your mail server. Telnet to your hostname or localhost with 25 following the host. The sendmail program will print a banner which will have the version number in it. You need to be running version 5.59. Version 5.61 will be released on Monday 12/12/1988. Any version less than 5.59 is a security problem.

   The following is a sample of the telnet command.

   ```
    % telnet localhost 25 Trying... Connected to lo-
   calhost.SEI.CMU.EDU. 220 ed.sei.cmu.edu Sendmail 5.59 ready at
   Wed, 7 Dec 88 15:45:55 EST Quit 221 ed.sei.cmu.edu closing connec-
   tion Connection closed by foreign host. %
   ```

2. Verify with your systems support staff that the ftpd program patches have been installed. Removing anonymous ftp is now known to NOT plug all security holes. If you are not sure, ftp to ucbarpa.berkeley.edu, login as anonymous password ftp and get ftpd.shar. This file contains the sources to the latest BSD release of the ftpd program.
3. Check your /etc/passwd file for bogus entries. Look for unauthorized accounts with the uid field set to zero (only the root account should have uid=0). Remove any unauthorized entries. The following is an example of what you might find.

   ```
    install::0:1::/:
   ```

   To check your /etc/passwd files for spurious accounts with uid 0, you can use the following awk program:

   ```
    % awk -F: '$3 == 0 {print $0}' /etc/passwd
   ```

   If you are running YP on your machine, do:

   ```
    % ypcat passwd | awk [...as above]
   ```

4. Look for modified /bin/login and /usr/ucb/telnet files. Several sites have found these programs with new "backdoors" added. Use the strings program to search /bin/login for the strings

OURPW, knaobj, and knaboj. If in doubt, reload the /bin/login and /usr/ucb/telnet executables from your distribution tape.

```
 % strings /bin/login | egrep '(OURPW|knaboj|knaobj)'
```

5. Educate your users to create hard to guess passwords. Account codes, first or last names, and common words are not very secure passwords. A few examples of common words are words that refer to your town, location, or company and words that are found in /usr/dict/words. Be especially careful of accounts where the password is the account name (easy to check, easy to guess).

6. In general, before you allow a user access to the Internet, you must be sure you know who they are. In other words, all users should be forced through a login/password sequence (no un-passworded accounts and preferably someplace which logs connections) before you let them get outside your local network. Be especially careful with TCP/IP terminal servers.

7. Check the last logs for normal logins as accounts which normally run utility programs (sync, who, etc), watch for unreasonable times.. watch for ftp's with funny logins (who, etc).

Revision History

```
September 16, 1997 Attached copyright statement
```