CERT Advisory CA-1993-10 Anonymous FTP Activity

Original issue date: July 14, 1993
Last revised: October 8, 1997
Attached copyright statement

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

The CERT Coordination Center has been receiving a continuous stream of reports from sites that are experiencing unwanted activities within their anonymous FTP areas. We recognize that this is not a new problem, and we have been striving to handle requests for assistance on a one-to-one basis with the reporting administrator. However, since this activity does not seem to be diminishing, CERT believes that a broad distribution of information concerning this problem and corresponding solution suggestions should help to address the widespread nature of this activity.

We are seeing three types of activity regarding anonymous FTP areas.

1. Improper configurations leading to system compromise.
2. Excessive transfer of data causing deliberate over-filling of disk space thus leading to denial of service.
3. Use of writable areas to transfer copyrighted software and other sensitive information.

This advisory provides an updated version of the anonymous FTP configuration guidelines that is available from CERT. The purpose of these guidelines is to assist system administrators at sites that offer anonymous FTP services. These guidelines are intended to aid a system administrator in configuring anonymous FTP capabilities so as to minimize unintended use of services or resources. Systems administrators should be aware that anonymous FTP capabilities should be configured and managed according to the policies established for their site.

You may obtain future copies of these guidelines through anonymous FTP from cert.org in ftp://ftp.cert.org/pub/tech_tips.

ANONYMOUS FTP CONFIGURATION GUIDELINES

Anonymous FTP can be a valuable service if correctly configured and administered. The first section of this document provides general guidance in initial configuration of an anonymous FTP area. The second section addresses the issues and challenges involved when a site wants to provide writable directories within their anonymous FTP areas. The third section provides information about previous CERT advisories related to FTP services.

The following guidelines are a set of suggested recommendations that have been beneficial to many sites. CERT recognizes that there will be sites that have unique requirements and needs, and that these sites may choose to implement different configurations.

1. Configuring anonymous FTP

    a. FTP daemon

    Sites should ensure that they are using the most recent version of their FTP daemon.

    a. Setting up the anonymous FTP directories

    The anonymous FTP root directory (~ftp) and its subdirectories should not be owned by the ftp account or be in the same group as the ftp account. This is a common configuration problem. If any of these directories are owned by ftp or are in the same group as the ftp account and are not write protected, an intruder will be able to add files (such as a .rhosts file) or modify other files. Many sites find it acceptable to use the root account. Making the ftp root directory and its subdirectories owned by root, part of the system group, and protected so that only root has write permission will help to keep your anonymous FTP service secure.

    Here is an example of an anonymous FTP directory setup:

```
drwxr-xr-x  7   root    system  512 Mar 1      15:17 ./
drwxr-xr-x 25   root    system  512 Jan 4      11:30 ../
drwxr-xr-x  2   root    system  512 Dec 20     15:43 bin/
drwxr-xr-x  2   root    system  512 Mar 12     16:23 etc/
drwxr-xr-x 10   root    system  512 Jun 5      10:54 pub/
```

    Files and libraries, especially those used by the FTP daemon and those in ~ftp/bin and ~ftp/etc, should have the same protections as these directories. They should not be owned by ftp or be in the same group as the ftp account; and they should be write protected.

    a. Using proper password and group files

    We strongly advise that sites not use the system's /etc/passwd file as the password file or the system's /etc/group as the group file in the ~ftp/etc directory. Placing these system files in the ~ftp/etc directory will permit intruders to get a copy of these files. These files are optional and are not used for access control.

    We recommend that you use a dummy version of both the ~ftp/etc/passwd and ~ftp/etc/group files. These files should be owned by root. The dir command uses these dummy versions to show owner and group names of the files and directories instead of displaying arbitrary numbers.

    Sites should make sure that the ~/ftp/etc/passwd file contains no account names that are the same as those in the system's /etc/passwd file. These files should include only those entries that are relevant to the FTP hierarchy or needed to show owner and group names. In addition, ensure that the password field has been cleared. The examples below show the use of asterisks (*) to clear the password field.

    Below is an example of a passwd file from the anonymous FTP area on cert.org:

```
ssphwg:*:3144:20:Site Specific Policy Handbook Working Group::
cops:*:3271:20:COPS Distribution::
cert:*:9920:20:CERT::
tools:*:9921:20:CERT Tools::
ftp:*:9922:90:Anonymous FTP::
nist:*:9923:90:NIST Files::
```

Here is an example group file from the anonymous FTP area on cert.org:

```
cert:*:20:
ftp:*:90:
```

1. Providing writable directories in your anonymous FTP configuration

   There is a risk to operating an anonymous FTP service that permits users to store files. CERT strongly recommends that sites do not automatically create a "drop off" directory unless thought has been given to the possible risks of having such a service. CERT has received many reports where these directories have been used as "drop off" directories to distribute bootlegged versions of copyrighted software or to trade information on compromised accounts and password files. CERT has also received numerous reports of files systems being maliciously filled causing denial of service problems.

   This section discusses three ways to address these problems. The first is to use a modified FTP daemon. The second method is to provide restricted write capability through the use of special directories. The third method involves the use of a separate directory.

   a. Modified FTP daemon

      If your site is planning to offer a "drop off" service, CERT suggests using a modified FTP daemon that will control access to the "drop off" directory. This is the best way to prevent unwanted use of writable areas. Some suggested modifications are:

      i. Implement a policy where any file dropped off cannot be accessed until the system manager examines the file and moves it to a public directory.
      ii. Limit the amount of data transferred in one session.
      iii. Limit the overall amount of data transferred based on available disk space.
      iv. Increase logging to enable earlier detection of abuses.

      For those interested in modifying the FTP daemon, source code is usually available from your vendor. Public domain sources are available from:

```
wuarchive.wustl.edu   ~ftp/packages/wuarchive-ftpd
ftp.uu.net            ~ftp/systems/unix/bsd-sources/libexec/ftpd
gatekeeper.dec.com    ~ftp/pub/DEC/gwtools/ftpd.tar.Z
```

      The CERT Coordination Center has not formally reviewed, evaluated, or endorsed the FTP daemons described. The decision to use the FTP daemons described is the responsibility of each user or organization, and we encourage each organization to thoroughly evaluate these programs before installation or use.

   a. Using protected directories

      If your site is planning to offer a "drop off" service and is unable to modify the FTP daemon, it is possible to control access by using a maze of protected directories. This method requires prior coordination and cannot guarantee protection from unwanted use of the writable FTP area, but has been used effectively by many sites.

      Protect the top level directory (~ftp/incoming) giving only execute permission to the anonymous user (chmod 751 ~ftp/incoming). This will permit the anonymous user to change directory (cd), but will not allow the user to view the contents of the directory.

```
drwxr-x--x  4   root    system  512 Jun 11      13:29 incoming/
```

      Create subdirectories in the ~ftp/incoming using names known only between your local users and the anonymous users that you want to have "drop off" permission. The same care used in selecting passwords should be taken in selecting these subdirectory names because the object is to choose names that cannot be easily guessed. Please do not use our example directory names of jAjwUth2 and MhaLL-iF.

```
drwxr-x-wx 10   root    system  512 Jun 11      13:54 jAjwUth2/
drwxr-x-wx 10   root    system  512 Jun 11      13:54 MhaLL-iF/
```

      This will prevent the casual anonymous FTP user from writing files in your anonymous FTP file system. It is important to realize that this method does not protect a site against the result of intentional or accidental disclosure of the directory names. Once a directory name becomes public knowledge, this method provides no protection at all from unwanted use of the area. Should a name become public, a site may choose to either remove or rename the writable directory.

   a. Using a single disk drive

      If your site is planning to offer a "drop off" service and is unable to modify the FTP daemon, it may be desirable to limit the amount of data transferred to a single file system mounted as ~ftp/incoming.

If possible, dedicate a disk drive and mount it as ~ftp/incoming. If this dedicated disk becomes full, it will not cause a denial of service problem.

The system administrator should monitor this directory (~ftp/incoming) on a continuing basis to ensure that it is not being misused.

1. Related CERT Advisories

   The following CERT Advisories directly relate to FTP daemons or impact on providing FTP service:

   CA-93.06.wuarchive.ftpd.vulnerability.
   CA-92.09.AIX.anonymous.ftp.vulnerability.
   CA-88.01.ftpd.hole

   Past advisories are available for anonymous FTP from cert.org.

Revision History

```
October 8, 1997  Attached copyright statement
```