CERT Advisory CA-1997-16 ftpd Signal Handling Vulnerability

Original issue date: May 29, 1997
Last revised: December 5, 1997
Added vendor information for NCR Corporation to the Updates section.

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

The text of this advisory was originally released by AUSCERT as AA-97.03 ftpd Signal Handling Vulnerability on January 29, 1997, and updated on April 18, 1997. To give this document wider distribution, we are reprinting the updated AUSCERT advisory here with their permission. Only the contact information at the end has changed: AUSCERT contact information has been replaced with CERT/CC contact information.

Although the text of the AUSCERT advisory has not changed, additional vendor information has been added immediately after the AUSCERT text.

We will update this advisory as we receive additional information. Look for it in an "Updates" section at the end of the advisory.

AUSCERT has received information that there is a vulnerability in some versions of ftpd distributed and installed under various Unix platforms.

This vulnerability may allow regular and anonymous ftp users to read or write to arbitrary files with root privileges.

The vulnerabilities in ftpd affect various third party and vendor versions of ftpd. AUSCERT recommends that sites take the steps outlined in section 3 as soon as possible.

This advisory will be updated as more information becomes available.

---

1. Description

AUSCERT has received information concerning a vulnerability in some vendor and third party versions of the Internet File Transfer Protocol server, ftpd(8).

This vulnerability is caused by a signal handling routine increasing process privileges to root, while still continuing to catch other signals. This introduces a race condition which may allow regular, as well as anonymous ftp, users to access files with root privileges. Depending on the configuration of the ftpd server, this may allow intruders to read or write to arbitrary files on the server.

This attack requires an intruder to be able to make a network connection to a vulnerable ftpd server.

Sites should be aware that the ftp services are often installed by default. Sites can check whether they are allowing ftp services by checking, for example, /etc/inetd.conf:

```
# grep -i '^ftp' /etc/inetd.conf
```

Note that on some systems the inetd configuration file may have a different name or be in a different location.
Please consult your documentation if the configuration file is not found in

/etc/inetd.conf.

If your site is offering ftp services, you may be able to determine the version of ftpd by checking the notice when first connecting.

The vulnerability status of specific vendor and third party ftpd servers can be found in Section 3.
Information involving this vulnerability has been made publicly available.

2. Impact

Regular and anonymous users may be able to access arbitrary files with root privileges. Depending on the configuration, this may allow anonymous, as well as regular, users to read or write to arbitrary files on the server with root privileges.

3. Workarounds/Solution

AUSCERT recommends that sites prevent the possible exploitation of this vulnerability by immediately applying vendor patches if they are available. Specific vendor information regarding this vulnerability is given in Section 3.1.

If the ftpd supplied by your vendor is vulnerable and no patches are available, sites may wish to install a third party ftpd which does not contain the vulnerability described in this advisory (Section 3.2).

3.1 Vendor patches

The following vendors have provided information concerning the vulnerability status of their ftpd distribution.
Detailed information has been appended in Appendix A. If your vendor is not listed below, you should contact your vendor directly.

Berkeley Software Design, Inc.
Digital Equipment Corporation
The FreeBSD Project
Hewlett-Packard Corporation
IBM Corporation
The NetBSD Project
The OpenBSD Project
Red Hat Software
Silicon Graphics Inc.
Washington University ftpd (Academ beta version)
Wietse Venema's logdaemon ftpd

3.2 Third party ftpd distributions

AUSCERT has received information that the following third party ftpd distributions do not contain the signal handling vulnerability described in this advisory:

wu-ftpd 2.4.2-beta-12
logdaemon 5.6 ftpd

Sites should ensure they are using the current version of this software. Information on these distributions is contained in Appendix A.

Sites should note that these third party ftpd distributions may offer some different functionality to vendor versions of ftpd. AUSCERT advises sites to read the documentation provided with the above third party ftpd distributions before installing.

Appendix A

Berkeley Software Design, Inc. (BSDI)

BSD/OS 2.1 is vulnerable to the ftpd problem described in this advisory. Patches have been issued and may be retrieved via the patches@BSDI.COM ema il server or from:

ftp://ftp.bsdi.com/bsdi/patches/patches-2.1/U210-033

Digital Equipment Corporation

DIGITAL UNIX Versions:

3.2c, 3.2de1, 3.2de2, 3.2f, 3.2g, 4.0, 4.0a, 4.0b

SOLUTION:

This potential security vulnerability has been resolved
and an official patch kit is available for DIGITAL UNIX V3.2g, V4.0, V4.0a, and V4.0b.

This article will be updated accordingly when patch kits for DIGITAL UNIX V3.2c, V3.2de1, V3.2de2, V3.2f become available.

The currently available patches may be obtained from your normal Digital support channel or from the following URL. (Select the appropriate version to locate this patch kit)

ftp://ftp.service.digital.com/patches/public/dunix

VERSION	KIT ID	SIZE	CHECK SUM	
v3.2g	SSRT0448U_v32g.tar	296960	32064	290
v4.0	SSRT0448U_v40.tar	542720	07434	530
v4.0a	SSRT0448U_v40a.tar	542720	43691	530
v4.0b	SSRT0448U_v40b.tar	471040	45701	460

Please refer to the applicable README notes information prior to the installation of patch kits on your system.

Note: The appropriate patch kit must be reinstalled following any upgrade beginning with V3.2c
up to and including V4.0b.

The FreeBSD Project

The FreeBSD Project has informed AUSCERT that the vulnerability described in this advisory has been fixed in FreeBSD-current (from January 27, 1997), and will be fixed in the upcoming FreeBSD 2.2 release. All previous versions of FreeBSD are vulnerable.

Hewlett-Packard Corporation

Hewlett-Packard has informed AUSCERT that the ftpd distributed with HP-UX 9.x and 10.x are vulnerable to this problem. Patches are currently in process.

IBM Corporation

The version of ftpd shipped with AIX is vulnerable to the conditions described in the advisory. The following APARs will be available shortly:

AIX 3.2 : APAR IX65536
AIX 4.1 : APAR IX65537
AIX 4.2 : APAR IX65538

To Order
APARs may be ordered using Electronic Fix Distribution (via FixDist) or from the IBM Support Center. For more information on FixDist, reference URL:

http://service.software.ibm.com/aixsupport/

or send e-mail to aixserv@austin.ibm.com with a subject of "FixDist".

The NetBSD Project
NetBSD (all versions) have the ftpd vulnerability described in this advisory. It has since been fixed in NetBSD-current. NetBSD have also made patches available and they can be retrieved from:

ftp://ftp.netbsd.org/pub/NetBSD/misc/security/19970123-ftpd

The OpenBSD Project
OpenBSD 2.0 did have the vulnerability described in this advisory, but has since been fixed in OpenBSD 2.0-current (from January 5, 1997).

Red Hat Software
The signal handling code in wu-ftpd has some security problems which allows users to read all files on your system. A new version of wu-ftpd is now available for Red Hat 4.0 which Red Hat suggests installing on all of your systems. This new version uses the same fix posted to redhat-list@redhat.com by Savochkin Andrey Vladimirovich. Users of Red Hat Linux versions earlier then 4.0 should upgrade to 4.0 and then apply all available security packages.

Users whose computers have direct internet connections may apply this update by using one of the following commands:

Intel:
rpm -Uvh ftp://ftp.redhat.com/updates/4.0/i386/wu-ftpd-2.4.2b11-9.i386.rpm

Alpha:
rpm -Uvh ftp://ftp.redhat.com/updates/4.0/axp/wu-ftpd-2.4.2b11-9.axp.rpm

SPARC:
rpm -Uvhftp://ftp.redhat.com/updates/4.0/sparc/wu-ftpd-2.4.2b11-9.sparc.rpm

All of these packages have been signed with Red Hat's PGP key.

wu-ftpd Academ beta version
The current version of wu-ftpd (Academ beta version), wu-ftpd 2.4.2-beta-12, does not contain the vulnerability described in this advisory. Sites using earlier versions should upgrade to the current version immediately. At the time of writing, the current version can be retrieved from:

ftp://ftp.academ.com/pub/wu-ftpd/private/

logdaemon Distribution
The current version of Wietse Venema's logdaemon (5.6) package contains an ftpd utility which addresses the vulnerability described in this advisory. Sites using earlier versions of this package should upgrade immediately. The current version of the logdaemon package can be retrieved from:

ftp://ftp.win.tue.nl/pub/security/ ftp://ftp.auscert.org.au/pub/mirrors/ftp.win.tue.nl/logdaemon/ ftp://ftp.cert.dfn.de/pub/tools/net/logdaemon/

The MD5 checksum for Version 5.6 of the logdaemon package is:

MD5 (logdaemon-5.6.tar.gz) = 5068f4214024ae56d180548b96e9f368

AUSCERT thanks David Greenman, Wietse Venema (visiting IBM T.J. Watson Research) and Stan Barber (Academ Consulting Services) for their contributions in finding solutions to this vulnerability. Thanks also to Dr Leigh Hume (Macquarie University), CERT/CC, and DFNCERT for their assistance in this matter. AUSCERT also thanks those vendors that provided feedback and patch information contained in this advisory.

UPDATES
Vendor Information Added by CERT/CC

Digital Equipment Corporation
AUG, 1997 DIGITAL UNIX Versions:

3.2C, 3.2DE1, 3.2DE2, 3.2F, 3.2G, 4.0, 4.0A, 4.0B, 4.0C

SOLUTION:

This potential security vulnerability has been resolved
and may be obtained from your normal Digital support channel or from the following URL.

NOTE: Previously released singular ECO patches
that were identified for this problem have been superseded in the aggregate versions
of the ECO patch kits.

ftp://ftp.service.digital.com/patches/public/dunix

(Select the appropriate version and it's aggregate patch kit).

Please refer to the applicable README notes information
prior to the installation of patch kits on your system.

Hewlett-Packard Corporation

HP has covered this in our security bulletin HPSBUX9702-055, 19 February 1997. The Security Bulletin contains pointers to the patches:

SOLUTION: Apply patch:

PHNE_10008 for all platforms with HP-UX releases 9.X
PHNE_10009 for all platforms with HP-UX releases 10.0X/10.10
PHNE_10010 for all platforms with HP-UX releases 10.20
PHNE_10011 for all platforms with HP-UX releases 10.20 (kftpd)

AVAILABILITY: All patches are available now.

IBM Corporation

See the appropriate release below to determine your action.

AIX 3.2

Apply the following fix to your system:

APAR - IX65536 (PTF - U447700)

To determine if you have this PTF on your system, run the following command:

lslpp -lB U447700

AIX 4.1

Apply the following fix to your system:

APAR - IX65537

To determine if you have this APAR on your system, run the following command:

instfix -ik IX65537

Or run the following command:

lslpp -h bos.net.tcp.client

Your version of bos.net.tcp.client should be 4.1.5.3 or later.

AIX 4.2

Apply the following fix to your system:

APAR - IX65538

To determine if you have this APAR on your system, run the following command:

instfix -ik IX65538

Or run the following command:

lslpp -h bos.net.tcp.client

Your version of bos.net.tcp.client should be 4.2.1.0 or later.

To Order

APARs may be ordered using Electronic Fix Distribution (via FixDist) or from the IBM Support Center. For more information on FixDist, reference URL:

http://service.software.ibm.com/aixsupport/

or send e-mail to aixserv@austin.ibm.com with a subject of "FixDist".

NCR Corporation

NCR is delivering a set of operating system dependent patches which contain an update for this problem. Accompanying each patch is a README file which discusses the general purpose of the patch and describes how to apply it to your system.

Recommended solution:

Apply one of the following patches depending on the revision of the inet package installed on your system. To check its version execute:

pkginfo -x inet

```
For inet 5.01.xx.xx: - PINET501 (Version later than 05.01.01.49)

For inet 6.01.xx.xx: - PINET601 (Version later than 06.01.00.06)

For inet 6.02.xx.xx: - Fix included in the product as shipped with
                       MP-RAS UNIX 3.02. (In inet package after
                       revision 6.02.00c).
```

Silicon Graphics Inc.

The ftpd program (/usr/etc/ftpd) is installed on all IRIX systems by default.

Patch information for this vulnerability is available in SGI"s Security Advisory 19970801-01-PX, "IRIX ftpd Signal Handling Vulnerability" available at

http://www.sgi.com/Support/Secur/security.html/

Sun Microsystems, Inc.

Not vulnerable.

Revision History

```
Dec. 5,  1997 Addedd vendor information for NCR Corporation to
              the Updates section.
Oct. 30, 1997 UPDATES, Vendor Information Added by CERT/CC -added information
              for NCR.
Sep. 30, 1997 Updated copyright statement
Aug. 15, 1997 Section 3.1 and UPDATES - Added by CERT/CC.Vendor patch information
 for Digital Equipment Corporation and Silicon Graphics, Inc.
June 3, 1997  Minor editorial formatting change.
June 9, 1997  UPDATES, Vendor Information Added by CERT/CC - added information
 for Sun Microsystems, Inc.
```