CERT Advisory CA-2000-13 Two Input Validation Problems In FTPD

Original release date: July 7, 2000
Last revised: November 21, 2000
Source: CERT/CC

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

Systems Affected

- Any system running wu-ftpd 2.6.0 or earlier
- Any system running ftpd derived from wu-ftpd 2.0 or later
- Some systems running ftpd derived from BSD ftpd 5.51 or BSD ftpd 5.60 (the final BSD release)

Overview

A vulnerability involving an input validation error in the "site exec" command has recently been identified in the Washington University ftpd (wu-ftpd) software package. Sites running affected systems are advised to update their wu-ftpd software as soon as possible.

A similar but distinct vulnerability has also been identified that involves a missing format string in several setproctitle() calls. It affects a broader number of ftp daemons. Please see
Appendix A of this document for specific information about the status of specific ftpd implementations and solutions.

I. Description

"Site exec" Vulnerability

A vulnerability has been identified in wu-ftpd and other ftp daemons based on the wu-ftpd source code. Wu-ftpd is a common package used to provide file transfer protocol (ftp) services. This vulnerability is being discussed as the wu-ftpd "site exec" or "lreply" vulnerability in various public forums. Incidents involving the exploitation of this vulnerabilitywhich enables remote users to gain root privilegeshave been reported to the CERT Coordination Center.

The problem is described in AUSCERT Advisory AA-2000.02, "wu-ftpd 'site exec' Vulnerability," which is available from

ftp://ftp.auscert.org.au/pub/auscert/advisory/AA-2000.02

The wu-ftpd "site exec" vulnerability is the result of missing character-formatting argument in several function calls that implement the "site exec" command functionality. Normally if "site exec" is enabled, a user logged into an ftp server (including the 'ftp' or 'anonymous' user) may execute a restricted subset of quoted commands on the server itself. However, if a malicious user can pass character format strings consisting of carefully constructed *printf() conversion characters (%f, %p, %n, etc) while executing a "site exec" command, the ftp daemon may be tricked into executing arbitrary code as root.

The "site exec" vulnerability appears to have been in the wu-ftpd code since the original wu-ftpd 2.0 came out in 1993. Any vendors who have based their own ftpd distributions on this vulnerable code are also likely to be vulnerable.

The vulnerability appears to be exploitable if a local user account can be used for ftp login. Also, if the "site exec" command functionality is enabled, then anonymous ftp login allows sufficient access for an attack.

setproctitle() Vulnerability

A separate vulnerability involving a missing character-formatting argument in setproctitle(), a call which sets the string used to display process identifier information, is also present in wu-ftpd. Other ftpd implementations have been found to have vulnerable setproctitle() calls as well, including those from proftpd and OpenBSD.

The setproctitle() vulnerability appears to have been present in various ftpd implementations since at least BSD ftpd 5.51 (which predates wuarchive-ftpd 1.0). It has also been confirmed to be present in BSD ftpd 5.60 (the final BSD release). Any vendors who have based their own ftpd distributions on this vulnerable code are also likely to be vulnerable.

It should be noted that many operating systems do not support setproctitle() calls. However, other software engineering defects involving the same type of missing character-formatting argument may be present.

It had been previously reported that the setproctitle() vulnerability had been used in conjunction with the "site exec" vulnerability to exploit vulnerable versions of wu-ftpd. The CERT/CC is unable to confirm such reports at this time.

Intruder Activity

One possible indication you are being attacked with either of these vulnerabilities may be the appearance of syslog entries similar to the following:

```
Jul  4 17:43:25 victim ftpd[3408]: USER ftp
Jul  4 17:43:25 victim ftpd[3408]: PASS [malicious shellcode]
Jul  4 17:43:26 victim ftpd[3408]: ANONYMOUS FTP LOGIN FROM
attacker.example.com [10.29.23.19], [malicious shellcode]
Jul  4 17:43:28 victim-site ftpd[3408]: SITE EXEC (lines: 0):
%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%
.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.
f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f
%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%
.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.
f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f
%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%c%c%c%.f|%p
Jul  4 17:43:28 victim ftpd[3408]: FTP session closed
```

Details of both the "site exec" and setproctitle() vulnerabilities have been posted in various public forums. Please see

http://www.securityfocus.com/vdb/bottom.html?section=discussion&vid=1387
http://www.securityfocus.com/vdb/bottom.html?section=discussion&vid=1425
http://ciac.llnl.gov/ciac/bulletins/k-054.shtml

The CERT/CC has received reports of the "site exec" vulnerability being successfully exploited on the Internet. Please check our Current Activity page for updates regarding intruder activity involving both of these vulnerabilities.

II. Impact

By exploiting any of these input validation problems, local or remote users logged into the ftp daemon may be able execute arbitrary code as root. An anonymous ftp user may also be able to execute arbitrary code as root.

III. Solution

Upgrade your version of ftpd

Please see Appendix A of this advisory for more information about the availability of updated ftpd packages specific for your system.

Apply a patch from your vendor

If you are running vulnerable ftpd implementations and cannot upgrade, you need to apply the appropriate vendor patches and recompile and/or reinstall the ftpd server software.

Appendix A contains information provided by vendors for this advisory. We will update the appendix as we receive more information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

Disable ftp services

If neither an upgrade nor a patch can be applied, the CERT/CC recommends disabling all vulnerable wu-ftpd and proftpd servers. While disabling "site exec" command functionality or anonymous ftp access minimizes exposure to the "site exec" vulnerability, neither is a complete solution and may not mitigate against the risks involved with exposure to the setproctitle() vulnerability.

Appendix A. Vendor Information

BSDI

Current versions of BSD/OS do not include any version of wu-ftpd. The BSDI ftpd is not vulnerable to the reported problems; it is not based on the wu-ftpd code.

The version of ftpd in modern versions of BSD/OS is not vulnerable to the generic setproctitle() vulnerabilities.

Caldera Systems, Inc

Please see CSSA-2000-020.0 regarding the wu-ftpd issue and OpenLinux:

ftp://ftp.calderasystems.com/pub/OpenLinux/security/CSSA-2000-020.0.txt

Copyright © 2000 Caldera Systems, Inc.

Conectiva S.A.

Please see:

http://www.securityfocus.com/templates/archive.pike?list =1&msg=20000623212826.A13925@conectiva.com.br

COMPAQ COMPUTER CORPORATION

At the time of writing this document, this reported problem is currently still under evaluation by engineering to determine the requirement of a solution if necessary. COMPAQ will provide an update to this advisory accordingly.

Debian GNU/Linux

Please see the following regarding the wu-ftpd "site exec" issue:

http://www.debian.org/security/2000/20000623

Copyright © 1997-2000 SPI

FreeBSD, Inc.

The version of ftpd shipped with all versions of FreeBSD since 2.2.0 is not vulnerable to this problem. FreeBSD also ships with several optional third-party FTP servers in the Ports Collection, including wu-ftpd and proftpd. The wu-ftpd vulnerability was corrected on 2000/06/24 and is the subject of FreeBSD Security Advisory SA-00:29. At this time no patch has been released by the proftpd vendor and the version in FreeBSD ports is still vulnerable to this attack. [An update to proftpd is now available. -CERT/CC] FreeBSD makes no guarantee about the security of third-party software in the ports collection and users are advised that there may be security vulnerabilities in other FTP servers available there.

Fujitsu

Fujitsu's UXP/V operating system is not vulnerable to any of the vulnerabilities discussed in [this] advisory.

Hewlett-Packard Company

HP is vulnerable. Please see:

HPSBUX0007-117: Sec. Vulnerability in ftpd, **Rev.01** HEWLETT-PACKARD COMPANY SECURITY ADVISORY: #00117, 11 July '00, Last Revised: 12 July '00

An excerpt:

PROBLEM: The ftp server (ftpd) on HP-UX allows users root access.

PLATFORM: HP-UX release 11.00 - Both Problem #1 and #2 below;
HP-UX release 10.20 - Problem #2, setproctitle(), only

DAMAGE: Unauthorized root access.

SOLUTION: Install temporary binary until an official patch is released.

AVAILABILITY: The temporary binary is available now (see below).

A. Background
There are 2 problems with FTP Server (ftpd) on HP-UX.

1. ftpd handling of the SITE EXEC command that allows remote users to gain root access. This is possible in the default configuration of ftpd on HP-UX 11.00 ONLY.
2. ftpd does not properly format the parameters to the setproctitle() function, allowing users to gain root access. This problem applies to both 11.00 and 10.X.

B. Fixing the problem
All system administrators are encouraged to install our temporary binary until an official patch is released. The file can be retrieved to simply replace the original factory supplied binary.

C. Recommended solution
Two temporary ftp binaries (for HP-UX 11.00 and HP-UX 10.20) can be found at:

ftp://ftp.cup.hp.com/dist/networking/ftp/ftpd.11.0
ftp://ftp.cup.hp.com/dist/networking/ftp/ftpd.10.20

Revised 01
--->>>These are to be installed in /usr/lbin/ftpd, with permissions 544.

NOTE: This advisory [HPSBUX0007-117] will be updated when patches become available.

Copyright © 2000 Hewlett-Packard Company

IBM Corporation

IBM's AIX operating system is not vulnerable to the exploit described in CA-2000-13

MandrakeSoft Inc.

Please see the MANDRAKE 7.1 update section for wu-ftpd information at:

http://www.linux-mandrake.com/en/fupdates.php3

Microsoft Coporation

The IIS FTP service is not is not affected by these issues.

MIT Kerberos Development Team

It seems that the MIT Kerberos ftpd is based on BSD ftpd revision 5.40, and has never contained any serious format string related bugs for some reason. It is possible that by defining an undocumented CPP macro SETPROCTITLE, calls to setproctitle() can be made, however, there is an internally declared setproctitle() function that does not take a format string as its argument, and is hence not vulnerable.

ProFTPD Project

Upgrade to ProFTPD 1.2.0:

http://www.proftpd.net/download.html

Please see the discussion concerning setproctitle() at

http://www.proftpd.org/proftpd-l-archive/00-07/msg00059.html
http://www.proftpd.org/proftpd-l-archive/00-07/msg00060.html
http://bugs.proftpd.net/show_bug.cgi?id=121
http://www.proftpd.net/security.html

NetBSD Foundation, Inc

Please see NetBSD Security Advisories NetBSD-SA2000-009 & NetBSD-SA2000-010:

ftp://ftp.NetBSD.ORG/pub/NetBSD/misc/security/advisories/NetBSD-SA2000-009.txt.asc
ftp://ftp.NetBSD.ORG/pub/NetBSD/misc/security/advisories/NetBSD-SA2000-010.txt.asc

Copyright © 2000, The NetBSD Foundation, Inc. All Rights Reserved.

OpenBSD

The setproctitle bug is in OpenBSD. Please see:

http://www.openbsd.org/errata.html#ftpd

Porcupine.org

[...] None of my software [ftpd from my logdaemon utilities] has either the "site exec" or "setproctitle" features enabled.

Wietse Venema
mailto:wietse@porcupine.org

Redhat

Please see RHSA-2000-039-02 regarding the wu-ftpd issue:

http://www.redhat.com/support/errata/RHSA-2000-039-02.html

Copyright © 2000 Red Hat, Inc. All rights reserved.

SGI

IRIX ftpd is not vulnerable to the issues mentioned in this advisory. See ftp://sgigate.sgi.com/security/20000701-01-I for more information.

Slackware Linux Project

Please see the patches made available regarding the wu-ftpd issue, at:

ftp://ftp.slackware.com/pub/slackware/slackware-7.1/patches/wu-ftpd-patch.README

Sun Microsystems

SISP FTPD is similar to wu-ftpd. SISP FTPD does not allow site exec nor does it use setproctitle(). Therefore, SISP FTPD does not appear to be vulnerable.

SuSE Ltd.

Please see SuSE Security Announcement #53 regarding the wu-ftpd issue, at:

http://www.suse.de/de/support/security/suse_security_announce_53.txt

WU-FTPD Development Group

The WU-FTPD Development Group's primary distribution site is mirrored world-wide. A list of mirrors is available from:

http://www.wu-ftpd.org/mirrors.txt

If possible, please use a mirror to obtain patches or the latest version.

Upgrade your version of wu-ftpd

The latest release of wu-ftpd, version 2.6.1, has been released to address these and several other security issues:

ftp://ftp.wu-ftpd.org

/pub/wu-ftpd/wu-ftpd-2.6.1.tar.gz

ftp://ftp.wu-ftpd.org/pub/wu-ftpd/wu-ftpd-2.6.1.tar.gz.asc

ftp://ftp.wu-ftpd.org/pub/wu-ftpd/wu-ftpd-2.6.1.tar.Z

ftp://ftp.wu-ftpd.org/pub/wu-ftpd/wu

-ftpd-2.6.1.tar.Z.asc

A

The wu-ftpd developers have published the following patch for wu-ftpd2.6.0: