CERT Advisory CA-1999-13 Multiple Vulnerabilities in WU-FTPD

Original release date: October 19, 1999
Last revised: November 9, 1999
Added vendor information for Fujitsu.
Source: CERT/CC

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

Systems Affected

- Systems running the WU-FTPD daemon or its derivatives

I. Description

Three vulnerabilities have 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. Incidents involving at least the first of these vulnerabilities have been reported to the CERT Coordination Center.

Vulnerability #1: MAPPING_CHDIR Buffer Overflow

Because of improper bounds checking, it is possible for an intruder to overwrite static memory in certain configurations of the WU-FTPD daemon. The overflow occurs in the MAPPING_CHDIR portion of the source code and is caused by creating directories with carefully chosen names. As a result, FTP daemons compiled without the MAPPING_CHDIR option are not vulnerable.

This is the same vulnerability described in AUSCERT Advisory AA-1999.01, which is available from

ftp://www.auscert.org.au/security/advisory/AA-1999.01.wu-ftpd.mapping_chdir.vul

This is not the same vulnerability as the one described in CA-99-03 "FTP Buffer Overflows", even though it is closely related. Systems that have patches to correct the issue described in CA-99-03 may still be vulnerable to this problem.

Vulnerability #2: Message File Buffer Overflow

Because of improper bounds checking during the expansion of macro variables in the message file, intruders may be able to overwrite the stack of the FTP daemon.

This is one of the vulnerabilities described in AUSCERT Advisory AA-1999.02, which is available from

ftp://www.auscert.org.au/security/advisory/AA-1999.02.multi.wu-ftpd.vuls

Vulnerability #3: SITE NEWER Consumes Memory

The SITE NEWER command is a feature specific to WUFTPD designed to allow mirroring software to identify all files newer than a supplied date. This command fails to free memory under some circumstances.

II. Impact

Vulnerability #1: MAPPING_CHDIR Buffer Overflow

Remote and local intruders may be able exploit this vulnerability to execute arbitrary code as the user running the ftpd daemon, usually root.

To exploit this vulnerability, the intruder must be able to create directories on the vulnerable systems that are accessible via FTP. While remote intruders are likely to have this privilege only through anonymous FTP access, local users may be able to create the required directories in their own home directories.

Vulnerability #2: Message File Buffer Overflow

Remote and local intruders may be able exploit this vulnerability to execute arbitrary code as the user running the ftpd daemon, usually root.

If intruders are able to control the contents of a message file, they can successfully exploit this vulnerability. This access is frequently available to local users in their home directories, but it may be restricted in anonymous FTP access, depending on your configuration.

Additionally, under some circumstances, remote intruders may be able to take advantage of message files containing macros provided by the FTP administrator.

Vulnerability #3: SITE NEWER Consumes Memory

Remote and local intruders who can connect to the FTP server can cause the server to consume excessive amounts of memory, preventing normal system operation. If intruders can create files on the system, they may be able exploit this vulnerability to execute arbitrary code as the user running the ftpd daemon, usually root.

III. Solution

Install appropriate patches from your vendor

These vulnerabilities can be eliminated by applying appropriate patches from your vendor. We encourage you to apply a patch as soon as possible and to disable vulnerable programs until you can do so.

Disabling the WU-FTPD daemon may prevent your system from operating normally. Upgrading to WU-FTPD 2.6.0 may cause some inter-operability problems with certain FTP clients. We encourage you to review the WU-FTPD documentation carefully before performing this upgrade.

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.

Until you can install a patch, you can apply the following workarounds.

Vulnerability #1: MAPPING_CHDIR Buffer Overflow

This vulnerability can be corrected by compiling the WU-FTPD daemon without the MAPPING_CHDIR option. Exploitation by anonymous remote intruders can be mitigated by limiting write access, but this solution is not encouraged.

Vulnerability #2: Message File Buffer Overflow

Remote exploitation of this vulnerability can be mitigated and possibly eliminated by removing macros from message files until a patch can be applied.

Vulnerability #3: SITE NEWER Consumes Memory

There are currently no workarounds available.

Appendix A. Vendor Information

Data General

DG/UX is not vulnerable to this problem.

FreeBSD

FreeBSD has updated its wuftpd and proftpd ports to correct this problem as of August 30, 1999. Users of these ports are encouraged to upgrade their installation to these newer versions of these ports as soon as possible.

Fujitsu

The Fujitsu UXP/V Operating System is not vulnerable.

IBM Corporation

AIX is not vulnerable. It does not ship wu-ftpd.

IBM and AIX are registered trademarks of International Business Machines Corporation.

OpenBSD

OpenBSD does not use (and never will use) wuftpd or any of its derivatives.

Santa Cruz Operation, Inc.

Security patches for SCO UnixWare 7.x, SCO UnixWare 2.x, and OpenServer 5.x will be made available at http://www.sco.com/security.

SGI

SGI IRIX and Unicos do not ship with wu-ftpd, so they are not vulnerable. As a courtesy, unsupported pre-compiled IRIX inst images for wu-ftpd are available from http://freeware.sgi.com/ which may be vulnerable. When the freeware products are next updated, they should contain the latest wu-ftpd code which should include the security fixes.

SGI Linux 1.0 which is based on RedHat 6.0 ships with wu-ftpd rpms. When new wu-ftpd rpms are available for RedHat 6.0, they can be installed on SGI Linux 1.0.

SGI NT Workstations do not ship with wu-ftpd.

Sun

Sun is not vulnerable.

WU-FTPD and BeroFTPD

Vulnerability #1:

Not vulnerable:
versions 2.4.2 and all betas and earlier versions
Vulnerable:
wu-ftpd-2.4.2-beta-18-vr4 through wu-ftpd-2.4.2-beta-18-vr15
wu-ftpd-2.4.2-vr16 and wu-ftpd-2.4.2-vr17
wu-ftpd-2.5.0
BeroFTPD, all versions

Vulnerability #2:

Not vulnerable:
wu-ftpd-2.6.0
Vulnerable:
All versions of wuarchive-ftpd and wu-ftpd prior to version 2.6.0, from wustl.edu, academ.com, vr.net and wu-ftpd.org.
BeroFTPD, all versions

Vulnerability #3:

Not vulnerable:
wu-ftpd-2.6.0
Vulnerable:
All versions of wuarchive-ftpd and wu-ftpd prior to version 2.6.0, from wustl.edu, academ.com, vr.net and wu-ftpd.org.
BeroFTPD, all versions

With version 2.6.0, the major functionality of BeroFTPD has been merged back into the WU-FTPD daemon. Development of BeroFTPD has ceased; there will be no upgrades or patches. Users are advised to upgrade to WU-FTPD version 2.6.0.

WU-FTPD Version 2.6.0 is available for download from mirrors arround the world. A full list of mirrors is available from:

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

The current version of WU-FTPD (presently 2.6.0) is also available from the primary distribution site:

ftp://ftp.wu-ftpd.org/pub/wu-ftpd/wu-ftpd-current.tar.gz
ftp://ftp.wu-ftpd.org/pub/wu-ftpd/wu-ftpd-current.tar.Z

The CERT Coordination Center would like to thank Gregory Lundberg (a member of the WU-FTPD development group) and AUSCERT their assistance in preparing this advisory.

Revision History

```
October 19, 1999  Initial release
November 9, 1999  Added vendor information for Fujitsu.
```