crashme

by Nightxade / Nightxade

Tags: buffer-overflow segfault pwn

Rating:

Can you make this program crash?
`nc 0.cloud.chals.io 17289`

crashme
crashme.c

We're given an ELF binary, a C source file, and a service to connect to. Here's `crashme.c`:

```c
#include <stdio.h>
#include <string.h>
#include <stdlib.h>

int main(int argc, char *argv[]){
    char buffer[32];
    printf("Give me some data: \n");
    fflush(stdout);
    fgets(buffer, 64, stdin);
    printf("You entered %s\n", buffer);
    fflush(stdout);
    return 0;
}
```

Seems like a very simple program. Simple programs require simple methods. `fgets()` can be vulnerable to buffer overflow, so why don't we try to send a large number of characters? I sent `aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa` to the local program, which immediately resulted in a `Segmentation fault`.

This is what we need then! Send the same input to the program to get the flag:

```
flag{segfaults_a_hackers_best_friend}
```

Original writeup (https://nightxade.github.io/ctf-writeups/writeups/2023/Cyber-Cooperative-CTF-2023/pwn/crashme.html).

Comments