[Bug] Use of uninitialized value in function wav_format_write in libwav.c #29

Open **tin-z** opened this issue on Mar 27 · 0 comments

tin-z commented on Mar 27

Describe the bug
An unitialized variable is used in function wav_format_write. The highest threat from this vulnerability is to data confidentiality.
The unitialized variable `format` is copied to the stream pointed by `f` variable, as illustrated below.

libwav/libwav.c
Lines 52 to 64 in `5cc8746`

```
52      enum wav_error
53      wav_format_write (const wav_format *format, FILE *f)
54      {
55              if (f == NULL)
56              {
57                      return WAV_FILE_NOT_OPENED;
58              }
59              else if (fwrite (format, sizeof (wav_format), 1, f) != 1)
60              {
61                      return WAV_ERROR;
62              }
63              return WAV_OK;
```

System info

- Ubuntu 20.04.3 LTS, clang version 12.0.1
- latest commit `5cc8746`

Steps to reproduce the behavior

- compile the program with UndefinedBehaviorSanitizer
- Run command: `./wav_gain POC /dev/null`

poc

https://github.com/tin-z/Stuff_and_POCs/blob/main/poc_libwav/POC

Output

```
Uninitialized bytes in __interceptor_fwrite at offset 0 inside [0x7ffed0df95e8, 16)
==273091==WARNING: MemorySanitizer: use-of-uninitialized-value
    #0 0x2ca7dc in wav_chunk_write
/dataZ/Part_2/libwav_example/libwav/tools/wav_gain/../../libwav.c
    #1 0x2cb559 in wav_write
/dataZ/Part_2/libwav_example/libwav/tools/wav_gain/../../libwav.c:217:2
    #2 0x2cb559 in gain_file /dataZ/Part_2/libwav_example/libwav/tools/wav_gain/wav_gain.c:28:6
    #3 0x2cb559 in main /dataZ/Part_2/libwav_example/libwav/tools/wav_gain/wav_gain.c:43:3
    #4 0x7f6b850e10b2 in __libc_start_main /build/glibc-sMfBJT/glibc-2.31/csu/../csu/libc-
start.c:308:16
    #5 0x24b43d in _start (/dataZ/Part_2/libwav_example/libwav/Fuzzing/wav_gain+0x24b43d)

SUMMARY: MemorySanitizer: use-of-uninitialized-value
/dataZ/Part_2/libwav_example/libwav/tools/wav_gain/../../libwav.c in wav_chunk_write
```

- Note, wav_chunk_write function calls wav_format_write, where it's the bug at.

tin-z changed the title ~~**Use of uninitialized value in function wav_format_write in libwav.c**~~ **[Bug] Use of uninitialized value in function wav_format_write in libwav.c** on Mar 28

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant