

New issue

Jump to bottom

heap-buffer-overflow in ok_csv_circular_buffer_read() at ok_csv.c:95 #13



aug5t7 opened this issue on Apr 29, 2021 · 3 comments

aug5t7 commented on Apr 29, 2021

Description

A heap-buffer-overflow was discovered in ok_file_formats. The issue is being triggered in function ok_csv_circular_buffer_read() at ok_csv.c:95

Version

dev version, git clone <https://github.com/brackeen/ok-file-formats.git>

Environment

Ubuntu 18.04, 64bit

Reproduce

test program

```
int main(int argc, char *argv[]) {
    FILE *file = fopen(argv[1], "rb");
    ok_csv *csv = ok_csv_read(file);
    fclose(file);
    if (csv->error_message) {
        fprintf(stderr, "%s\n", csv->error_message);
    }
    ok_csv_free(csv);
    return 0;
}
```

Compile test program with Address Sanitizer:

```
gcc -g -fsanitize=address main-asan main.c ok_csv.c ok_csv.h
```

Asan Report

```
$ ./main-asan ./poc.csv
=====
==58179==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x606000000480 at pc 0x7f4834e5577a bp 0x7fff1198aed0 sp 0x7fff1198a678
WRITE of size 181 at 0x606000000480 thread T0
#0 0x7f4834e55779 in (/usr/lib/x86_64-linux-gnu/libasan.so.4+0x79779)
#1 0x55fd598bd79a in ok_csv_circular_buffer_read /home/au9/ok-file-format/ok_csv.c:95
#2 0x55fd598bf52d in ok_csv_decode2 /home/au9/ok-file-format/ok_csv.c:484
#3 0x55fd598bdf1d in ok_csv_decode /home/au9/ok-file-format/ok_csv.c:241
#4 0x55fd598bdd4a in ok_csv_read /home/au9/ok-file-format/ok_csv.c:177
#5 0x55fd598bd0c2 in main /home/au9/ok-file-format/main.c:8
#6 0x7f4834a0cbf6 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21bf6)
#7 0x55fd598bcf89 in _start (/home/au9/ok-file-format/main-asan+0xf89)

0x606000000480 is located 0 bytes to the right of 64-byte region [0x606000000440,0x606000000480)
allocated by thread T0 here:
#0 0x7f4834e4b40 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0x4deb40)
#1 0x55fd598bf4e1 in ok_csv_decode2 /home/au9/ok-file-format/ok_csv.c:479
#2 0x55fd598bdf1d in ok_csv_decode /home/au9/ok-file-format/ok_csv.c:241
#3 0x55fd598bdd4a in ok_csv_read /home/au9/ok-file-format/ok_csv.c:177
#4 0x55fd598bd0c2 in main /home/au9/ok-file-format/main.c:8
#5 0x7f4834a0cbf6 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21bf6)

SUMMARY: AddressSanitizer: heap-buffer-overflow (/usr/lib/x86_64-linux-gnu/libasan.so.4+0x79779)
Shadow bytes around the buggy address:
 0x0c0c7fff8040: 00 00 00 00 00 00 03 fa fa fa 00 00 00 00
 0x0c0c7fff8050: 00 00 00 05 fa fa fa 00 00 00 00 00 05 fa
 0x0c0c7fff8060: fa fa fa 00 00 00 00 00 04 fa fa fa fa
 0x0c0c7fff8070: 00 00 00 00 00 00 06 fa fa fa 00 00 00 00
 0x0c0c7fff8080: 00 00 00 05 fa fa fa 00 00 00 00 00 00 00
=>0x0c0c7fff8090:[fa]fa fa fa fa fa fa fa fa fa
 0x0c0c7fff80a0: fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c0c7fff80b0: fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c0c7fff80c0: fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c0c7fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c0c7fff80e0: fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
Addressable: 00
Partially addressable: 01 02 03 04 05 06 07
Heap left redzone: fa
Freed heap region: fd
Stack left redzone: f1
Stack mid redzone: f2
Stack right redzone: f3
Stack after return: f5
Stack use after scope: f8
Global redzone: f9
Global init order: f6
Poisoned by user: f7
Container overflow: fc
Array cookie: ac
Intra object redzone: bb
```

```
ASan internal:      fe
Left alloca redzone: ca
Right alloca redzone: cb
==58179==ABORTING
```

PoC

[poc.csv](#)

 **brackeen** added a commit that referenced this issue on Apr 29, 2021


 **ok_csv**: Fix circular buffer reading (#13)

4713de3

brackeen commented on Apr 29, 2021

Owner

Thanks, @AugJube, this is now fixed

 **brackeen** closed this as completed on Apr 29, 2021

xxrz commented on Nov 15, 2021

Hi, @aug5t7 ~ ,May I get your contact e-mail? I would like to ask some questions about submitting CVE. I would be very grateful if you can take the time to reply to me!

aug5t7 commented on Nov 17, 2021 • edited

Author

Hi, @aug5t7 ~ ,May I get your contact e-mail? I would like to ask some questions about submitting CVE. I would be very grateful if you can take the time to reply to me!

Contact me at au9st7@gmail.com .

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants

