SEGV in function bmp_load at bmp.c:57 #22

Open **xiaoxiongwang** opened this issue on May 23, 2020 · 3 comments

xiaoxiongwang commented on May 23, 2020

Tested in Ubuntu 16.04, 64bit.

The testcase is segv_ffjpeg_e1.

I use the following command:

```
ffjpeg -e segv_ffjpeg_e1
```

and get:

```
Segmentation fault
```

I use **valgrind** to analysis the bug and get the below information (absolute path information omitted):

```
==15595== Memcheck, a memory error detector
==15595== Copyright (C) 2002-2015, and GNU GPL'd, by Julian Seward et al.
==15595== Using Valgrind-3.11.0 and LibVEX; rerun with -h for copyright info
==15595== Command: ffjpeg -e segv_ffjpeg_e
==15595==
==15595== Invalid write of size 1
==15595==    at 0x4C35035: __GI_mempcpy (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==15595==    by 0x4EB303D: _IO_file_xsgetn (fileops.c:1392)
==15595==    by 0x4EA8235: fread (iofread.c:38)
==15595==    by 0x4016D9: fread (stdio2.h:295)
==15595==    by 0x4016D9: bmp_load (bmp.c:57)
==15595==    by 0x400F2B: main (ffjpeg.c:29)
==15595==  Address 0x852060cf is not stack'd, malloc'd or (recently) free'd
==15595==
==15595==
==15595== Process terminating with default action of signal 11 (SIGSEGV)
==15595==  Access not within mapped region at address 0x852060CF
==15595==    at 0x4C35035: __GI_mempcpy (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==15595==    by 0x4EB303D: _IO_file_xsgetn (fileops.c:1392)
==15595==    by 0x4EA8235: fread (iofread.c:38)
==15595==    by 0x4016D9: fread (stdio2.h:295)
==15595==    by 0x4016D9: bmp_load (bmp.c:57)
==15595==    by 0x400F2B: main (ffjpeg.c:29)
==15595==  If you believe this happened as a result of a stack
==15595==  overflow in your program's main thread (unlikely but
==15595==  possible), you can try to increase the size of the
==15595==  main thread stack using the --main-stacksize= flag.
==15595==  The main thread stack size used in this run was 8388608.
==15595==
==15595== HEAP SUMMARY:
==15595==     in use at exit: 3,624 bytes in 2 blocks
==15595==   total heap usage: 3 allocs, 1 frees, 7,720 bytes allocated
==15595==
==15595== LEAK SUMMARY:
==15595==    definitely lost: 0 bytes in 0 blocks
==15595==    indirectly lost: 0 bytes in 0 blocks
==15595==      possibly lost: 0 bytes in 0 blocks
==15595==    still reachable: 3,624 bytes in 2 blocks
==15595==         suppressed: 0 bytes in 0 blocks
==15595== Rerun with --leak-check=full to see details of leaked memory
==15595==
==15595== For counts of detected and suppressed errors, rerun with: -v
==15595== ERROR SUMMARY: 1 errors from 1 contexts (suppressed: 0 from 0)
Segmentation fault
```

I use **AddressSanitizer** to build ffjpeg and running it with the following command:

```
ffjpeg -e segv_ffjpeg_e1
```

This is the ASAN information (absolute path information omitted):

```
ASAN:SIGSEGV
=================================================================
==16256==ERROR: AddressSanitizer: SEGV on unknown address 0x61f08000fa20 (pc 0x7fdcba5a8443 bp 0x000000000240 sp 0x7ffe28f759f8 T0)
    #0 0x7fdcba5a8442  (/lib/x86_64-linux-gnu/libc.so.6+0x8f442)
    #1 0x7fdcba59203d  (/lib/x86_64-linux-gnu/libc.so.6+0x7903d)
    #2 0x7fdcba587235 in _IO_fread (/lib/x86_64-linux-gnu/libc.so.6+0x6e235)
    #3 0x401670 in bmp_load ffjpeg/src/bmp.c:57
    #4 0x401294 in main (ffjpeg/src/ffjpeg+0x401294)
    #5 0x7fdcba53982f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
    #6 0x4010c8 in _start (ffjpeg/src/ffjpeg+0x4010c8)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV ??:0 ??
==16256==ABORTING
```

An attacker can exploit this vulnerability by submitting a malicious bmp that exploits this bug which will result in a Denial of Service (DoS).

xiaoxiongwang commented on May 29, 2020 • edited Author

CVE-2020-13440 has been assigned to this issue.The link is here.

rockcarry added a commit that referenced this issue on Jul 27, 2020

`fix issue #22.` e63a75f

rockcarry commented on Jul 27, 2020 Owner

new commit `e63a75f` fix this issue
@xiaoxiongwang please check and test.

myztaoislland commented on May 21

The testcase is lost, **@xiaoxiongwang** could you please upload again?

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants