New issue

Jump to bottom

heap overflow in stb_image.h:2099 #1108

Closed **Kaka201** opened this issue on Mar 4, 2021 · 2 comments

Labels 1 stb_image 2 bug w/ repro **5 merged-dev** priority

Kaka201 commented on Mar 4, 2021

heap overflow by a craft jpeg file in stb_image.h:2099
poc poc_hoob.zip

asan report:

```
==42271==ERROR: AddressSanitizer: global-buffer-overflow on address 0x000000559f20 at pc 0x00000051a2dd bp 0x7ffd06a9e900 sp 0x7ffd06a9e8f8
READ of size 4 at 0x000000559f20 thread T0
    #0 0x51a2dc in stbi__extend_receive /home/kaka/fuzz/stb/tests/./../stb_image.h:2099:16
    #1 0x518400 in stbi__jpeg_decode_block /home/kaka/fuzz/stb/tests/./../stb_image.h:2154:15
    #2 0x517173 in stbi__parse_entropy_coded_data /home/kaka/fuzz/stb/tests/./../stb_image.h:2920:30
    #3 0x5138d0 in stbi__decode_jpeg_image /home/kaka/fuzz/stb/tests/./../stb_image.h:3321:15
    #4 0x510a21 in load_jpeg_image /home/kaka/fuzz/stb/tests/./../stb_image.h:3773:9
    #5 0x4fe7b1 in stbi__jpeg_load /home/kaka/fuzz/stb/tests/./../stb_image.h:3930:13
    #6 0x4f8b3f in stbi__load_and_postprocess_8bit /home/kaka/fuzz/stb/tests/./../stb_image.h:1203:19
    #7 0x4f9d12 in stbi_load_from_memory /home/kaka/fuzz/stb/tests/./../stb_image.h:1373:11
    #8 0x4fd734 in LLVMFuzzerTestOneInput /home/kaka/fuzz/stb/tests/stbi_read_fuzzer.c:19:26
    #9 0x4f84fd in main /home/kaka/fuzz/stb/tests/fuzz_main.c:48:11
    #10 0x7fd09b4ea83f in __libc_start_main /build/glibc-e6zv40/glibc-2.23/csu/../csu/libc-start.c:291
    #11 0x41b038 in _start (/home/kaka/fuzz/stb/tests/image_fuzzer+0x41b038)

0x000000559f20 is located 32 bytes to the left of global variable '<string literal>' defined in './../stb_image.h:2198:33' (0x559f40) of size 22
  '<string literal>' is ascii string 'can't merge dc and ac'
0x000000559f20 is located 0 bytes to the right of global variable 'stbi__jbias' defined in './../stb_image.h:2083:18' (0x559ee0) of size 64
SUMMARY: AddressSanitizer: global-buffer-overflow /home/kaka/fuzz/stb/tests/./../stb_image.h:2099:16 in stbi__extend_receive
Shadow bytes around the buggy address:
  0x0000800a3390: 00 04 f9 f9 f9 f9 f9 00 04 f9 f9 f9 f9 f9
  0x0000800a33a0: 00 f9 f9 f9 f9 f9 f9 00 00 01 f9 f9 f9 f9
  0x0000800a33b0: 00 00 00 00 00 00 00 00 04 f9 f9 f9 f9 f9
  0x0000800a33c0: 00 00 00 00 00 00 00 00 00 00 02 f9 f9 f9
  0x0000800a33d0: 00 00 00 00 00 00 00 02 f9 f9 f9 f9 00 00
=>0x0000800a33e0: 00 00 00 00[f9]f9 f9 f9 00 00 06 f9 f9 f9
  0x0000800a33f0: 00 04 f9 f9 f9 f9 f9 f9 00 00 05 f9 f9 f9
  0x0000800a3400: 00 06 f9 f9 f9 f9 f9 00 05 f9 f9 f9 f9 f9
  0x0000800a3410: 00 00 04 f9 f9 f9 f9 f9 00 02 f9 f9 f9 f9
  0x0000800a3420: 00 00 f9 f9 f9 f9 f9 f9 00 00 02 f9 f9 f9
  0x0000800a3430: 00 00 05 f9 f9 f9 f9 f9 00 06 f9 f9 f9 f9
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
  Shadow gap:              cc
==42271==ABORTING
```

rygorous added 1 stb_image 2 bug w/ repro priority labels on Jun 28, 2021

rygorous added a commit that referenced this issue on Jul 2, 2021

`stb_image: Fix bug on JPEGs with malformed DC deltas` ··· `a3f2897`

rygorous commented on Jul 2, 2021 Collaborator

Thanks for the bug report and repro, sorry for taking a while to respond. Bug is fixed in dev branch, will be in the next release.

rygorous added the **5 merged-dev** label on Jul 2, 2021

rygorous added a commit that referenced this issue on Jul 4, 2021

`stb_image: Fix bug on JPEGs with malformed DC deltas` ··· `86b7570`

nothings closed this as completed on Jul 11, 2021

Kaka201 commented on Oct 14, 2021 Author

CVE-2021-28021 has been assigned for this issue
report by luo likang from nsfocus security team

Assignees

No one assigned

Labels

1 stb_image 2 bug w/ repro **5 merged-dev** priority

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants