New issue

Jump to bottom

heap-use-after-free at MagickCore/pixel-accessor.h in GetPixelRed #1723

Closed 3 tasks done **SuhwanSong** opened this issue on Oct 6, 2019 · 4 comments

Labels bug

Milestone 7.0.9-0

SuhwanSong commented on Oct 6, 2019

Prerequisites

- [x] I have written a descriptive issue title
- [x] I have verified that I am using the latest version of ImageMagick
- [x] I have searched open and closed issues to ensure it has not already been reported

Description

There is a heap-use-after-free at MagickCore/pixel-accessor.h:378:10 in GetPixelRed

Steps to Reproduce

poc
please run a following cmd with poc file.

```
magick $PoC -despeckle -flip -monochrome -alpha Shape tmp.rla
```

Here's ASAN log.

```
==8370==ERROR: AddressSanitizer: heap-use-after-free on address 0x62a000024200 at pc 0x000000796779 bp 0x7ffdf7956b10 sp 0x7ffdf7956b08
READ of size 4 at 0x62a000024200 thread T0
    #0 0x796778 in GetPixelRed ImageMagick/./MagickCore/pixel-accessor.h:378:10
    #1 0x7938d7 in GetPixelIntensity ImageMagick/MagickCore/pixel.c:2367:24
    #2 0x258de7a in SetImageAlphaChannel ImageMagick/MagickCore/channel.c:1298:28
    #3 0x625776b in CLISimpleOperatorImage ImageMagick/MagickWand/operation.c:1765:18
    #4 0x6250c70 in CLISimpleOperatorImages ImageMagick/MagickWand/operation.c:3685:12
    #5 0x632eddb in CLIOption ImageMagick/MagickWand/operation.c:5302:16
    #6 0x5588f52 in ProcessCommandOptions ImageMagick/MagickWand/magick-cli.c:477:7
    #7 0x55910cc in MagickImageCommand ImageMagick/MagickWand/magick-cli.c:796:5
    #8 0x559b0e3 in MagickCommandGenesis ImageMagick/MagickWand/mogrify.c:185:14
    #9 0x51c3e5 in MagickMain ImageMagick/utilities/magick.c:149:10
    #10 0x519c69 in main ImageMagick/utilities/magick.c:180:10
    #11 0x7fdc4a357b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:310
    #12 0x421849 in _start (magick+0x421849)

0x62a000024200 is located 0 bytes inside of 22592-byte region [0x62a000024200,0x62a000029a40)
freed by thread T0 here:
    #0 0x4e1530 in __interceptor_free.localalias.0 (magick+0x4e1530)
    #1 0x6c76f0 in RelinquishAlignedMemory ImageMagick/MagickCore/memory.c:1037:3
    #2 0x245efb2 in RelinquishPixelCachePixels ImageMagick/MagickCore/cache.c:974:40
    #3 0x24e304f in OpenPixelCache ImageMagick/MagickCore/cache.c:3762:19
    #4 0x2506bd7 in GetImagePixelCache ImageMagick/MagickCore/cache.c:1757:18
    #5 0x2533d59 in SyncImagePixelCache ImageMagick/MagickCore/cache.c:5501:28
    #6 0x2601f04 in SetImageColorspace ImageMagick/MagickCore/colorspace.c:1244:10
    #7 0x2609fa7 in TransformsRGBImage ImageMagick/MagickCore/colorspace.c:1981:11
    #8 0x2605cc8 in TransformImageColorspace ImageMagick/MagickCore/colorspace.c:1407:12
    #9 0x70c801 in ConformPixelInfo ImageMagick/MagickCore/pixel.c:232:12
    #10 0x258da15 in SetImageAlphaChannel ImageMagick/MagickCore/channel.c:1294:9
    #11 0x625776b in CLISimpleOperatorImage ImageMagick/MagickWand/operation.c:1765:18
    #12 0x6250c70 in CLISimpleOperatorImages ImageMagick/MagickWand/operation.c:3685:12
    #13 0x632eddb in CLIOption ImageMagick/MagickWand/operation.c:5302:16
    #14 0x5588f52 in ProcessCommandOptions ImageMagick/MagickWand/magick-cli.c:477:7
    #15 0x55910cc in MagickImageCommand ImageMagick/MagickWand/magick-cli.c:796:5
    #16 0x559b0e3 in MagickCommandGenesis ImageMagick/MagickWand/mogrify.c:185:14
    #17 0x51c3e5 in MagickMain ImageMagick/utilities/magick.c:149:10
    #18 0x519c69 in main ImageMagick/utilities/magick.c:180:10
    #19 0x7fdc4a357b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:310

previously allocated by thread T0 here:
    #0 0x4e2338 in __interceptor_posix_memalign (magick+0x4e2338)
    #1 0x6bcd6a in AcquireAlignedMemory ImageMagick/MagickCore/memory.c:265:7
    #2 0x24e0cbd in OpenPixelCache ImageMagick/MagickCore/cache.c:3733:46
    #3 0x2506bd7 in GetImagePixelCache ImageMagick/MagickCore/cache.c:1757:18
    #4 0x2533d59 in SyncImagePixelCache ImageMagick/MagickCore/cache.c:5501:28
    #5 0x56d7ad in SetImageStorageClass ImageMagick/MagickCore/image.c:2625:10
    #6 0x258d244 in SetImageAlphaChannel ImageMagick/MagickCore/channel.c:1266:14
    #7 0x625776b in CLISimpleOperatorImage ImageMagick/MagickWand/operation.c:1765:18
    #8 0x6250c70 in CLISimpleOperatorImages ImageMagick/MagickWand/operation.c:3685:12
    #9 0x632eddb in CLIOption ImageMagick/MagickWand/operation.c:5302:16
    #10 0x5588f52 in ProcessCommandOptions ImageMagick/MagickWand/magick-cli.c:477:7
    #11 0x55910cc in MagickImageCommand ImageMagick/MagickWand/magick-cli.c:796:5
    #12 0x559b0e3 in MagickCommandGenesis ImageMagick/MagickWand/mogrify.c:185:14
    #13 0x51c3e5 in MagickMain ImageMagick/utilities/magick.c:149:10
    #14 0x519c69 in main ImageMagick/utilities/magick.c:180:10
    #15 0x7fdc4a357b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:310

SUMMARY: AddressSanitizer: heap-use-after-free ImageMagick/./MagickCore/pixel-accessor.h:378:10 in GetPixelRed
Shadow bytes around the buggy address:
  0x0c547fffc7f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c547fffc800: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c547fffc810: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c547fffc820: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c547fffc830: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c547fffc840:[fd]fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c547fffc850: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
```

```
  0x0c547fffc860: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c547fffc870: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c547fffc880: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c547fffc890: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
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
==8370==ABORTING
```

System Configuration

- ImageMagick version:
  Version: ImageMagick 7.0.8-68 Q16 x86_64 2019-10-06 https://imagemagick.org
- Environment (Operating system, version and so on):
  Description: Ubuntu 18.04.1 LTS
  Release: 18.04
  Codename: bionic
- Additional information:
  CC=clang-6 CXX=clang++-6 CFLAGS="-fsanitize=address,undefined -g" CXXFLAGS="-fsanitize=address,undefined -g" ./configure --disable-openmp

urban-warrior commented on Oct 6, 2019 — Contributor

Thanks for the problem report. We can reproduce it and will have a patch to fix it in GIT master branch @ https://github.com/ImageMagick/ImageMagick later today. The patch will be available in the beta releases of ImageMagick @ https://www.imagemagick.org/download/beta/ by sometime tomorrow.

dlemstra added the bug label on Oct 6, 2019

dlemstra added this to the **7.0.8-69** milestone on Oct 6, 2019

dlemstra closed this as completed on Oct 27, 2019

tcullum-rh commented on Oct 28, 2020

@urban-warrior Cristy, does the fix for #1724 also fix this? It looks like it could be the same bug and I notice there's not a commit attached to this one directly. I'm not intimately familiar with ImageMagick code but the similarity between the call stacks makes it seem like it could be.

Thanks!

urban-warrior commented on Oct 28, 2020 — Contributor

Yes. We attached the commit to the #1724 and you can see these are same bug its just occurs a few lines down. The red pixel rather than the blue pixel.

tcullum-rh commented on Oct 28, 2020

@urban-warrior Thank you for letting me know! :)

rtfingc mentioned this issue on Mar 21, 2021

Poc of ImageMagick SuhwanSong/PoC#1

Open

Assignees

No one assigned

Labels

bug

Milestone

7.0.9-0

Development

No branches or pull requests

4 participants