AddressSanitizer: heap-buffer-overflow /src/imagemagick/./MagickCore/quantum-private.h:256:27 in PushLongPixel #4988

✓ Closed **salmonx** opened this issue on Mar 25 · 3 comments

salmonx commented on Mar 25 • edited ▾

ImageMagick version

7.1.0-27

Operating system

Linux

Operating system, version and so on

Linux d477f3580ae9 5.4.0-105-generic #119~18.04.1-Ubuntu SMP Tue Mar 8 11:21:24 UTC 2022 x86_64 x86_64 x86_64 GNU/Linux

Description

Hello,
We are currently working on fuzz testing feature, and we found a heap-use-after-free on ImageMagick.

Steps to Reproduce

```
➜  oss-fuzz git:(master) ✗ python infra/helper.py reproduce imagemagick encoder_cin_fuzzer
./build/out/imagemagick/crash-772bceeffddfb027f3363fb5be34fa55195a6e1a
INFO:root:Running: docker run --rm --privileged -i -v /work/fuzz/oss-
fuzz/build/out/imagemagick:/out -v /work/fuzz/oss-fuzz/build/out/imagemagick/crash-
772bceeffddfb027f3363fb5be34fa55195a6e1a:/testcase -t gcr.io/oss-fuzz-base/base-runner reproduce
encoder_cin_fuzzer -runs=100.
+ FUZZER=encoder_cin_fuzzer
+ shift
+ '[' '!' -v TESTCASE ']'
+ TESTCASE=/testcase
+ '[' '!' -f /testcase ']'
+ export RUN_FUZZER_MODE=interactive
+ RUN_FUZZER_MODE=interactive
+ export FUZZING_ENGINE=libfuzzer
+ FUZZING_ENGINE=libfuzzer
+ export SKIP_SEED_CORPUS=1
+ SKIP_SEED_CORPUS=1
+ run_fuzzer encoder_cin_fuzzer -runs=100 /testcase
/out/encoder_cin_fuzzer -rss_limit_mb=2560 -timeout=25 -runs=100 /testcase -close_fd_mask=3 <
/dev/null
INFO: Running with entropic power schedule (0xFF, 100).
INFO: Seed: 543797506
INFO: Loaded 1 modules   (228899 inline 8-bit counters): 228899 [0x1f6a8b0, 0x1fa26d3),
INFO: Loaded 1 PC tables (228899 PCs): 228899 [0x1fa26d8,0x2320908),
/out/encoder_cin_fuzzer: Running 1 inputs 100 time(s) each.
Running: /testcase
=================================================================
==18==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61b000001408 at pc 0x000000c77cfc
bp 0x7ffd2026fd90 sp 0x7ffd2026fd88
READ of size 1 at 0x61b000001408 thread T0
SCARINESS: 12 (1-byte-read-heap-buffer-overflow)
    #0 0xc77cfb in PushLongPixel /src/imagemagick/./MagickCore/quantum-private.h:256:27
    #1 0xc77cfb in ImportRGBQuantum /src/imagemagick/MagickCore/quantum-import.c:4061:15
    #2 0xc77cfb in ImportQuantumPixels /src/imagemagick/MagickCore/quantum-import.c:4774:7
    #3 0xd8a7e0 in ReadCINImage /src/imagemagick/coders/cin.c:774:12
    #4 0x9cfca1 in ReadImage /src/imagemagick/MagickCore/constitute.c:728:15
    #5 0x94d996 in BlobToImage /src/imagemagick/MagickCore/blob.c:475:13
    #6 0x81e2b1 in Magick::Image::read(Magick::Blob const&)
/src/imagemagick/Magick++/lib/Image.cpp:4043:12
    #7 0x7ea865 in LLVMFuzzerTestOneInput /src/imagemagick/Magick++/fuzz/encoder_fuzzer.cc:66:11
    #8 0x6e0502 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long) /src/llvm-
project/compiler-rt/lib/fuzzer/FuzzerLoop.cpp:611:15
    #9 0x6cb462 in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned long) /src/llvm-
project/compiler-rt/lib/fuzzer/FuzzerDriver.cpp:324:6
    #10 0x6d0ccc in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char const*, unsigned
long)) /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerDriver.cpp:860:9
    #11 0x6fa2b2 in main /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerMain.cpp:20:10
    #12 0x7f40139740b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x240b2)
    #13 0x6a9bad in _start (/out/encoder_cin_fuzzer+0x6a9bad)

DEDUP_TOKEN: PushLongPixel--ImportRGBQuantum--ImportQuantumPixels
0x61b000001408 is located 0 bytes to the right of 1416-byte region [0x61b000000e80,0x61b000001408)
allocated by thread T0 here:
    #0 0x7e678d in operator new[](unsigned long) /src/llvm-project/compiler-
rt/lib/asan/asan_new_delete.cpp:98:3
    #1 0x810ed0 in Magick::BlobRef::BlobRef(void const*, unsigned long)
/src/imagemagick/Magick++/lib/BlobRef.cpp:30:12
    #2 0x80ff7d in Magick::Blob::Blob(void const*, unsigned long)
/src/imagemagick/Magick++/lib/Blob.cpp:27:18
    #3 0x7ea859 in LLVMFuzzerTestOneInput /src/imagemagick/Magick++/fuzz/encoder_fuzzer.cc:64:22
    #4 0x6e0502 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long) /src/llvm-
project/compiler-rt/lib/fuzzer/FuzzerLoop.cpp:611:15
    #5 0x6cb462 in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned long) /src/llvm-
project/compiler-rt/lib/fuzzer/FuzzerDriver.cpp:324:6
    #6 0x6d0ccc in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char const*, unsigned
long)) /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerDriver.cpp:860:9
    #7 0x6fa2b2 in main /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerMain.cpp:20:10
    #8 0x7f40139740b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x240b2)

DEDUP_TOKEN: operator new[](unsigned long)--Magick::BlobRef::BlobRef(void const*, unsigned long)--Magick::Blob::Blob(void const*, unsigned long)
SUMMARY: AddressSanitizer: heap-buffer-overflow /src/imagemagick/./MagickCore/quantum-private.h:256:27 in PushLongPixel
Shadow bytes around the buggy address:
  0x0c367fff8230: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c367fff8240: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c367fff8250: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c367fff8260: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c367fff8270: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c367fff8280: 00[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c367fff8290: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c367fff82a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c367fff82b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c367fff82c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c367fff82d0: fa fa fa 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
==18==ABORTING
```

Images

poc.zip

urban-warrior commented on Mar 25 Contributor

Unfortunately we cannot reproduce the issue with the `main` branch. Both `valgrind` and `clang -fsanitize=address,undefined` do not return memory exceptions for

```
magick crash-772bceeffddfb027f3363fb5be34fa55195a6e1a null:
```

salmonx mentioned this issue on Mar 25

Unable to reproduce the heap-buffer-overflow bug in ImageMagick encoder_cin_fuzzer?
google/oss-fuzz#7457

Closed

salmonx commented on Mar 26 • edited ▾ Author

@urban-warrior

```
root@2573fe874425:/src/imagemagick# convert images/crash-772bceeffddfb027f3363fb5be34fa55195a6e1a
xxx.png
convert-im6.q16: unexpected end-of-file `images/crash-772bceeffddfb027f3363fb5be34fa55195a6e1a':
No such file or directory @ error/cin.c/ReadCINImage/787.
root@2573fe874425:/src/imagemagick# ll images/crash-772bceeffddfb027f3363fb5be34fa55195a6e1a
-rw-r--r-- 1 root root 1416 Mar 26 11:16 images/crash-772bceeffddfb027f3363fb5be34fa55195a6e1a
```

urban-warrior pushed a commit that referenced this issue on Mar 26

https://github.com/ImageMagick/ImageMagick/issues/4988 ✓ ca3654e

urban-warrior pushed a commit to ImageMagick/ImageMagick6 that referenced this issue on Mar 26

https://github.com/ImageMagick/ImageMagick/issues/4988 ✓ e6ea587

urban-warrior commented on Mar 26 Contributor

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

👍 1

netbsd-srcmastr pushed a commit to NetBSD/pkgsrc that referenced this issue on Apr 20

`ImageMagick: update to 7.1.30` … d355f7c

dlemstra closed this as completed on Apr 30

Assignees

No one assigned

Labels

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants