ImageMagick / ImageMagick Public

<> Code ⊙ Issues 115 Pull requests 1 Discussions Actions Wiki •••

New issue

Jump to bottom

heap-buffer-overflow in magick at quantum-private.h PushShortPixel #4974

Closed **fa1lr4in** opened this issue on Mar 21 · 1 comment

fa1lr4in commented on Mar 21 • edited ▾

ImageMagick version

7.1.0-28

Operating system

Linux

Operating system, version and so on

OS: Ubuntu 20.04.3 LTS
Version: ImageMagick 7.1.0-28 Q16-HDRI x86_64 2022-03-04 https://imagemagick.org
Copyright: (C) 1999 ImageMagick Studio LLC
License: https://imagemagick.org/script/license.php
Features: Cipher DPC HDRI
Delegates (built-in): bzlib fontconfig freetype jbig jng jpeg lzma pangocairo png tiff x xml zlib
Compiler: gcc (4.2)

Description

Hello,
We found a heap overflow vulnerability in magick

Steps to Reproduce

build it

```
CC=afl-clang-lto CXX=afl-clang-lto++ CFLAGS="-g -fsanitize=address -fno-omit-frame-pointer" CXXFLAGS="-g -fsanitize=address -fno-omit-frame-pointer" LDFLAGS="-g -fsanitize=address -fno-omit-frame-pointer" ./configure --disable-shared --prefix="/root/fuzz/target/imagemagick/ImageMagick/install"
```

```
AFL_USE_ASAN=1 make -j24 && make install -j24
```

run it

```
./magick convert poc /dev/null
```

output

```
=================================================================
==1195823==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61900000181c at pc 0x000000cd5328 bp 0x7ffdacd61fa0 sp 0x7ffdacd61f98
READ of size 1 at 0x61900000181c thread T0
#0 0xcd5327 in PushShortPixel /root/fuzz/target/image_magick/ImageMagick/./MagickCore/quantum-private.h
#1 0xcd5327 in ImportRGBAQuantum /root/fuzz/target/image_magick/ImageMagick/MagickCore/quantum-import.c:4232:15
#2 0xcd5327 in ImportQuantumPixels /root/fuzz/target/image_magick/ImageMagick/MagickCore/quantum-import.c:4780:7
#3 0x13e73f2 in ReadTIFFImage /root/fuzz/target/imagemagick/ImageMagick/coders/tiff.c:2052:24
#4 0x6f9981 in ReadImage /root/fuzz/target/image_magick/ImageMagick/MagickCore/constitute.c:728:15
#5 0x6fe991 in ReadImages /root/fuzz/target/image_magick/ImageMagick/MagickCore/constitute.c:1075:9
#6 0x157caa5 in ConvertImageCommand /root/fuzz/target/imagemagick/ImageMagick/MagickWand/convert.c:614:18
#7 0x17191fd in MagickCommandGenesis /root/fuzz/target/imagemagick/ImageMagick/MagickWand/mogrify.c:188:14
#8 0x580b89 in MagickMain /root/fuzz/target/imagemagick/ImageMagick/utilities/magick.c:150:10
#9 0x580b89 in main /root/fuzz/target/imagemagick/ImageMagick/utilities/magick.c:182:10
#10 0x7f499b68b0b2 in __libc_start_main /build/glibc-sMfBJT/glibc-2.31/csu/../csu/libc-start.c:308:16
#11 0x4ce36d in _start (/root/fuzz/target/imagemagick/ImageMagick/install/bin/magick+0x4ce36d)

0x61900000181c is located 10 bytes to the right of 914-byte region [0x619000001480,0x619000001812)
allocated by thread T0 here:
#0 0x54ab1d in malloc (/root/fuzz/target/imagemagick/ImageMagick/install/bin/magick+0x54ab1d)
#1 0x13e6faf in ReadTIFFImage /root/fuzz/target/imagemagick/ImageMagick/coders/tiff.c:1996:39
#2 0x6f9981 in ReadImage /root/fuzz/target/image_magick/ImageMagick/MagickCore/constitute.c:728:15
#3 0x6fe991 in ReadImages /root/fuzz/target/image_magick/ImageMagick/MagickCore/constitute.c:1075:9
#4 0x157caa5 in ConvertImageCommand /root/fuzz/target/imagemagick/ImageMagick/MagickWand/convert.c:614:18
#5 0x17191fd in MagickCommandGenesis /root/fuzz/target/imagemagick/ImageMagick/MagickWand/mogrify.c:188:14
#6 0x580b89 in MagickMain /root/fuzz/target/imagemagick/ImageMagick/utilities/magick.c:150:10
#7 0x580b89 in main /root/fuzz/target/imagemagick/ImageMagick/utilities/magick.c:182:10
#8 0x7f499b68b0b2 in __libc_start_main /build/glibc-sMfBJT/glibc-2.31/csu/../csu/libc-start.c:308:16
```

```
SUMMARY: AddressSanitizer: heap-buffer-overflow
/root/fuzz/target/image_magick/ImageMagick/./MagickCore/quantum-private.h in PushShortPixel
Shadow bytes around the buggy address:
0x0c327fff82b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c327fff82c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c327fff82d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c327fff82e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c327fff82f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c327fff8300: 00 00 02[fa]fa fa fa fa fa fa fa fa fa fa fa fa
0x0c327fff8310: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c327fff8320: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c327fff8330: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c327fff8340: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c327fff8350: 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
==1195823==ABORTING
```

Images

poc.zip

urban-warrior pushed a commit to ImageMagick/ImageMagick6 that referenced this issue on Mar 22

`https://github.com/ImageMagick/ImageMagick/issues/4974` ✓ `1f860f5`

urban-warrior pushed a commit that referenced this issue on Mar 22 `https://github.com/ImageMagick/ImageMagick/issues/4974` ✓ `c871830`

urban-warrior commented on Mar 22 — 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.

urban-warrior closed this as completed on Mar 23

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

`ImageMagick: update to 7.1.30` … `d355f7c`

Assignees

No one assigned

Labels

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants