lvandeve / lodepng Public

Code Issues 50 Pull requests 25 Actions Projects Wiki ···

New issue

Jump to bottom

SEGV on unknown address in function pngdetail. #177

Closed yangfar opened this issue on Oct 21 · 2 comments

yangfar commented on Oct 21

Version

pngdetail by Lode Vandevenne
version: 20220717

Command

./pngdetail @@

Crash Output

```
AddressSanitizer:DEADLYSIGNAL
```

```
=================================================================
==2262494==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000003 (pc 0x0000004f43b4 bp 0x000000000080 sp 0x7ffd35c4f320 T0)
==2262494==The signal is caused by a WRITE memory access.
==2262494==Hint: address points to the zero page.
#0 0x4f43b4 in readChunk_tRNS(LodePNGColorMode*, unsigned char const*, unsigned long) /home/hjsz/fuzz_software/lodepng-master/lodepng.cpp:4406:65
#1 0x4f2716 in lodepng_inspect_chunk(LodePNGState*, unsigned long, unsigned char const*, unsigned long) /home/hjsz/fuzz_software/lodepng-master/lodepng.cpp:4793:13
#2 0x5a39c0 in inspect_chunk_by_name(unsigned char const*, unsigned char const*, lodepng::State&, char const*) /home/hjsz/fuzz_software/lodepng-master/pngdetail.cpp:155:10
#3 0x5a39c0 in Data::loadInspect() /home/hjsz/fuzz_software/lodepng-master/pngdetail.cpp:221:7
#4 0x591e19 in showHeaderInfo(Data&, Options const&) /home/hjsz/fuzz_software/lodepng-master/pngdetail.cpp:1109:8
#5 0x59db24 in showInfos(Data&, Options const&) /home/hjsz/fuzz_software/lodepng-master/pngdetail.cpp:1330:79
#6 0x5a12a6 in main /home/hjsz/fuzz_software/lodepng-master/pngdetail.cpp:1444:5
#7 0x7fd0de890082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/csu/../csu/libc-start.c:308:16
#8 0x41d76d in _start (/home/hjsz/fuzz_software/lodepng-master/pngdetail+0x41d76d)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/hjsz/fuzz_software/lodepng-master/lodepng.cpp:4406:65 in readChunk_tRNS(LodePNGColorMode*, unsigned char const*, unsigned long)
==2262494==ABORTING
```

POC

POC.zip
Report of the Information Security Laboratory of Ocean University of China @OUC_ISLOUC @OUC_Blue_Whale

Thanks for your time!

feliwir commented 18 days ago

@lvandeve this appears inside the nist database: https://nvd.nist.gov/vuln/detail/CVE-2022-44081

Could you maybe take a deeper look at this?

lvandeve commented 18 days ago • edited ▾ Owner

Thanks for discovering this issue and reporting! It's fixed with 997936fd2b45842031e4180d73d7880e381cf33f

The issue was in the binary utility pngdetail.cpp instead of the library itself, and was due to not correctly checking all errors

👍 2

lvandeve closed this as completed 18 days ago

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants