

\_\_\_\_\_\_

- ==2262494==ERROR: AddressSanitizer: SEGV on unknown address 0x00000000003 (pc 0x00000004f43b4 bp 0x0000000000080 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-Szlz7B/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

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

Could you maybe take a deeper look at this?

Ivandeve 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





Assignees		
No one assigned		
Labels		
None yet		
Projects		
None yet		
Milestone		
No milestone		
Development		
No branches or pull requests		
3 participants		





