New issue

Jump to bottom

BUGS FOUND #41

Open **Cvjark** opened this issue on Jun 29 · 0 comments

Cvjark commented on Jun 29 • edited

hi, with the help of fuzzing ,I found some crash sample in this repo.
crash sample will be offered, and to reproduce the crash info please use command `./linux/jpegdec crash_sample`

negative-size-param

sample here:

negative-size-param-crash-sample.zip

crash info:

```
--11053-- ERROR: AddressSanitizer: negative-size-param: (size=-555)
    #0 0x4ad750 in __asan_memcpy /home/bupt/Desktop/tools/llvm-12.0.1/llvm/projects/compiler-rt/lib/asan/asan_interceptors_memintrinsics.cpp:22
    #1 0x5138a0 in JPEGParseInfo /home/bupt/Desktop/JPEGDEC/linux/./../src/jpeg.inl:1381:17
    #2 0x512866 in main /home/bupt/Desktop/JPEGDEC/linux/main.c:42:14
    #3 0x7f1585cabc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-start.c:310
    #4 0x41c109 in _start (/home/bupt/Desktop/JPEGDEC/linux/jpegdec+0x41c109)

0x0000010136aa is located 6602 bytes inside of global variable 'jpg' defined in 'main.c:14:11' (0x1011ce0) of size 17864
SUMMARY: AddressSanitizer: negative-size-param /home/bupt/Desktop/tools/llvm-12.0.1/llvm/projects/compiler-rt/lib/asan/asan_interceptors_memintrinsics.cpp:22 in __asan_memcpy
==11053==ABORTING
```

SEGV on unknown address

sample1:

SEGV on unknown address sample1.zip

crash info:

```
AddressSanitizer:DEADLYSIGNAL
--16536-- ERROR: AddressSanitizer: SEGV on unknown address 0x000050538315 (pc 0x000000519856 bp
0x000000000001 sp 0x7ffda97ee2f0 T0)
--16536-- The signal is caused by a READ memory access.
    #0 0x519856 in TIFFSHORT /home/bupt/Desktop/JPEGDEC/linux/./../src/jpeg.inl
    #1 0x519856 in GetTIFFInfo /home/bupt/Desktop/JPEGDEC/linux/./../src/jpeg.inl:1191:17
    #2 0x516242 in JPEGParseInfo /home/bupt/Desktop/JPEGDEC/linux/./../src/jpeg.inl:1425:29
    #3 0x512866 in main /home/bupt/Desktop/JPEGDEC/linux/main.c:42:14
    #4 0x7ff45c6c4c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #5 0x41c109 in _start (/home/bupt/Desktop/JPEGDEC/linux/jpegdec+0x41c109)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/bupt/Desktop/JPEGDEC/linux/./../src/jpeg.inl in TIFFSHORT
==16536==ABORTING
```

sample2:

SEGV on unknown address sample2.zip

crash info:

```
AddressSanitizer:DEADLYSIGNAL
==53466==ERROR: AddressSanitizer: SEGV on unknown address 0x000700000080 (pc 0x7f9ea1731c01 bp
0x000000014538 sp 0x7ffefc49da70 T0)
==53466==The signal is caused by a READ memory access.
    #0 0x7f9ea1731c01 in fseek /build/glibc-CVJwZb/glibc-2.27/libio/fseek.c:35
    #1 0x4f49d4 in seekFile /home/bupt/Desktop/JPEGDEC/linux/./../src/jpeg.inl:645:5
    #2 0x51381a in JPEGParseInfo /home/bupt/Desktop/JPEGDEC/linux/./../src/jpeg.inl:1375:17
    #3 0x512866 in main /home/bupt/Desktop/JPEGDEC/linux/main.c:42:14
    #4 0x7f9ea16cbc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #5 0x41c109 in _start (/home/bupt/Desktop/JPEGDEC/linux/jpegdec+0x41c109)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /build/glibc-CVJwZb/glibc-2.27/libio/fseek.c:35 in fseek
==53466==ABORTING
```

global-buffer-overflow

crash sample1:

global-buffer-overflow-crash-sample1.zip

crash info:

```
==53474==ERROR: AddressSanitizer: global-buffer-overflow on address 0x00000101b880 at pc
0x00000050f80b bp 0x7ffe917d20f0 sp 0x7ffe917d20e8
WRITE of size 1 at 0x00000101b880 thread T0
    #0 0x50f80a in JPEGPutMCU8BitGray /home/bupt/Desktop/JPEGDEC/linux/./../src/jpeg.inl:2026:26
    #1 0x50f80a in DecodeJPEG /home/bupt/Desktop/JPEGDEC/linux/./../src/jpeg.inl:3428:17
    #2 0x51298c in JPEG_decode /home/bupt/Desktop/JPEGDEC/linux/./../src/jpeg.inl:577:12
    #3 0x51298c in main /home/bupt/Desktop/JPEGDEC/linux/main.c:50:6
    #4 0x7f7afe6f8c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #5 0x41c109 in _start (/home/bupt/Desktop/JPEGDEC/linux/jpegdec+0x41c109)

0x00000101b880 is located 1120 bytes to the right of global variable 'ucDitherBuffer' defined in
'main.c:15:9' (0x1017420) of size 16384
SUMMARY: AddressSanitizer: global-buffer-overflow
/home/bupt/Desktop/JPEGDEC/linux/./../src/jpeg.inl:2026:26 in JPEGPutMCU8BitGray
Shadow bytes around the buggy address:
  0x0000801fb6c0: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
  0x0000801fb6d0: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
  0x0000801fb6e0: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
  0x0000801fb6f0: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
  0x0000801fb700: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
=>0x0000801fb710:[f9]f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
  0x0000801fb720: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
  0x0000801fb730: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
  0x0000801fb740: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
  0x0000801fb750: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
  0x0000801fb760: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
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
  Shadow gap:              cc
```

```
==53474==ABORTING
info: No menu item '=' in node '(dir)Top'
```

crash sample2：

global-buffer-overflow-crash-sample2.zip

crash info：

```
==53494==ERROR: AddressSanitizer: global-buffer-overflow on address 0x0000010162f0 at pc
0x00000051b8f7 bp 0x7ffd42bca940 sp 0x7ffd42bca938
READ of size 2 at 0x0000010162f0 thread T0
    #0 0x51b8f6 in JPEGDecodeMCU /home/bupt/Desktop/JPEGDEC/linux/./../src/jpeg.inl:1704:22
    #1 0x4f741a in DecodeJPEG /home/bupt/Desktop/JPEGDEC/linux/./../src/jpeg.inl:3326:20
    #2 0x51298c in JPEG_decode /home/bupt/Desktop/JPEGDEC/linux/./../src/jpeg.inl:577:12
    #3 0x51298c in main /home/bupt/Desktop/JPEGDEC/linux/main.c:50:6
    #4 0x7fe142af9c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #5 0x41c109 in _start (/home/bupt/Desktop/JPEGDEC/linux/jpegdec+0x41c109)

0x0000010162f0 is located 72 bytes to the right of global variable 'jpg' defined in 'main.c:14:11'
(0x1011ce0) of size 17864
SUMMARY: AddressSanitizer: global-buffer-overflow
/home/bupt/Desktop/JPEGDEC/linux/./../src/jpeg.inl:1704:22 in JPEGDecodeMCU
Shadow bytes around the buggy address:
  0x0000801fac00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0000801fac10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0000801fac20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0000801fac30: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0000801fac40: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0000801fac50: 00 00 00 00 00 f9 f9 f9 f9 f9 f9 f9 f9 f9[f9]f9
  0x0000801fac60: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
  0x0000801fac70: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
  0x0000801fac80: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
  0x0000801fac90: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
  0x0000801faca0: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
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
  Shadow gap:              cc
==53494==ABORTING
```

FPE

crash sample1:

FPE-sample1.zip

crash info:

```
AddressSanitizer:DEADLYSIGNAL

==53478==ERROR: AddressSanitizer: FPE on unknown address 0x0000004f6aa6 (pc 0x0000004f6aa6 bp
0x7ffd10d4a3d0 sp 0x7ffd10d49c40 T0)
    #0 0x4f6aa6 in DecodeJPEG /home/bupt/Desktop/JPEGDEC/linux/./../src/jpeg.inl:3285:37
    #1 0x51298c in JPEG_decode /home/bupt/Desktop/JPEGDEC/linux/./../src/jpeg.inl:577:12
    #2 0x51298c in main /home/bupt/Desktop/JPEGDEC/linux/main.c:50:6
    #3 0x7f92f93acc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #4 0x41c109 in _start (/home/bupt/Desktop/JPEGDEC/linux/jpegdec+0x41c109)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: FPE /home/bupt/Desktop/JPEGDEC/linux/./../src/jpeg.inl:3285:37 in
DecodeJPEG
==53478==ABORTING
```

crash sample2:

FPE-sample2.zip

crash info:

```
AddressSanitizer:DEADLYSIGNAL

==53482==ERROR: AddressSanitizer: SEGV on unknown address 0x00004f4a7e15 (pc 0x000000519856 bp
0x000000000001 sp 0x7ffed5dd5f70 T0)
==53482==The signal is caused by a READ memory access.
    #0 0x519856 in TIFFSHORT /home/bupt/Desktop/JPEGDEC/linux/./../src/jpeg.inl
    #1 0x519856 in GetTIFFInfo /home/bupt/Desktop/JPEGDEC/linux/./../src/jpeg.inl:1191:17
    #2 0x516242 in JPEGParseInfo /home/bupt/Desktop/JPEGDEC/linux/./../src/jpeg.inl:1425:29
    #3 0x512866 in main /home/bupt/Desktop/JPEGDEC/linux/main.c:42:14
    #4 0x7f5efd945c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
```

```
    #5 0x41c109 in _start (/home/bupt/Desktop/JPEGDEC/linux/jpegdec+0x41c109)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/bupt/Desktop/JPEGDEC/linux/./../src/jpeg.inl in TIFFSHORT
==53482==ABORTING
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant