# BUGS FOUND #10

Open **Cvjark** opened this issue on Jun 30 · 0 comments

**Cvjark** commented on Jun 30 • edited

hi, i found something unusual in this repo, are they new bugs ?
To reproduce the crash please use command: `./png_demo @@ /dev/null (replace @@ to the sample's path)`

## FPE

### crash sample

id0-FPE-sample1.zip

### crash info

```
AddressSanitizer:DEADLYSIGNAL
==22761==ERROR: AddressSanitizer: FPE on unknown address 0x0000004f4665 (pc 0x0000004f4665 bp
0x7fffaf2c27f0 sp 0x7fffaf2c19e0 T0)
    #0 0x4f4665 in SaveBMP(char*, unsigned char*, unsigned char*, int, int, int)
/home/bupt/Desktop/PNGdec/linux/main.cpp:56:21
    #1 0x4f5311 in main /home/bupt/Desktop/PNGdec/linux/main.cpp:144:9
    #2 0x7f42d9d84c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #3 0x41c129 in _start (/home/bupt/Desktop/PNGdec/linux/png_demo+0x41c129)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: FPE /home/bupt/Desktop/PNGdec/linux/main.cpp:56:21 in SaveBMP(char*,
unsigned char*, unsigned char*, int, int, int)
==22761==ABORTING
```

## heap-buffer-overflow

### crash sample No.1

id1-heap-buffer-overflow-sample1.zip

## crash info of sample No.1

```
==22802==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000000011 at pc
0x00000043b61c bp 0x7ffefb2a1690 sp 0x7ffefb2a0e40
READ of size 40 at 0x602000000011 thread T0
    #0 0x43b61b in __interceptor_fwrite.part.57 /home/bupt/Desktop/tools/llvm-
12.0.1/llvm/projects/compiler-
rt/lib/asan/../sanitizer_common/sanitizer_common_interceptors.inc:1143
    #1 0x4f491a in SaveBMP(char*, unsigned char*, unsigned char*, int, int, int)
/home/bupt/Desktop/PNGdec/linux/main.cpp:89:13
    #2 0x4f5311 in main /home/bupt/Desktop/PNGdec/linux/main.cpp:144:9
    #3 0x7f0ed9adfc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #4 0x41c129 in _start (/home/bupt/Desktop/PNGdec/linux/png_demo+0x41c129)

0x602000000011 is located 0 bytes to the right of 1-byte region [0x602000000010,0x602000000011)
allocated by thread T0 here:
    #0 0x4ae6f0 in malloc /home/bupt/Desktop/tools/llvm-12.0.1/llvm/projects/compiler-
rt/lib/asan/asan_malloc_linux.cpp:145
    #1 0x4f51ec in main /home/bupt/Desktop/PNGdec/linux/main.cpp:128:34

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/bupt/Desktop/tools/llvm-
12.0.1/llvm/projects/compiler-
rt/lib/asan/../sanitizer_common/sanitizer_common_interceptors.inc:1143 in
__interceptor_fwrite.part.57
Shadow bytes around the buggy address:
  0x0c047fff7fb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c047fff8000: fa fa[01]fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8010: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8020: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8050: 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
  Shadow gap:              cc
==22802==ABORTING
```

## crash sample No.2

id2-heap-buffer-overflow-sample2.zip

## crash info of sample No.2

```
==22853==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6220000017b0 at pc
0x0000004ad554 bp 0x7ffc9c610730 sp 0x7ffc9c60fee0
WRITE of size 132 at 0x6220000017b0 thread T0
    #0 0x4ad553 in __asan_memcpy /home/bupt/Desktop/tools/llvm-12.0.1/llvm/projects/compiler-
rt/lib/asan/asan_interceptors_memintrinsics.cpp:22
    #1 0x4fc310 in DecodePNG(png_image_tag*, void*, int)
/home/bupt/Desktop/PNGdec/linux/../src/png.inl:801:33
    #2 0x4fc310 in PNG::decode(void*, int)
/home/bupt/Desktop/PNGdec/linux/../src/PNGdec.cpp:194:12
    #3 0x4f5207 in main /home/bupt/Desktop/PNGdec/linux/main.cpp:129:18
    #4 0x7f6fa7b19c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #5 0x41c129 in _start (/home/bupt/Desktop/PNGdec/linux/png_demo+0x41c129)

0x6220000017b0 is located 0 bytes to the right of 5808-byte region [0x622000000100,0x6220000017b0)
allocated by thread T0 here:
    #0 0x4ae6f0 in malloc /home/bupt/Desktop/tools/llvm-12.0.1/llvm/projects/compiler-
rt/lib/asan/asan_malloc_linux.cpp:145
    #1 0x4f51ec in main /home/bupt/Desktop/PNGdec/linux/main.cpp:128:34

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/bupt/Desktop/tools/llvm-
12.0.1/llvm/projects/compiler-rt/lib/asan/asan_interceptors_memintrinsics.cpp:22 in __asan_memcpy
Shadow bytes around the buggy address:
  0x0c447fff82a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c447fff82b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c447fff82c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c447fff82d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c447fff82e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c447fff82f0: 00 00 00 00 00 00[fa]fa fa fa fa fa fa fa fa
  0x0c447fff8300: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c447fff8310: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c447fff8320: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c447fff8330: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c447fff8340: 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
  Shadow gap:              cc
==22853==ABORTING
```

## crash sample No.3

id8-heap-buffer-overflow-sample3.zip

## crash info of sample No.3

```
==23090==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7fad078fceb2 at pc
0x0000004f4e69 bp 0x7ffe0c9898b0 sp 0x7ffe0c9898a8
READ of size 1 at 0x7fad078fceb2 thread T0
    #0 0x4f4e68 in SaveBMP(char*, unsigned char*, unsigned char*, int, int, int)
/home/bupt/Desktop/PNGdec/linux/main.cpp:84:24
    #1 0x4f5311 in main /home/bupt/Desktop/PNGdec/linux/main.cpp:144:9
    #2 0x7fad0ae1dc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #3 0x41c129 in _start (/home/bupt/Desktop/PNGdec/linux/png_demo+0x41c129)

0x7fad078fceb2 is located 2 bytes to the right of 2013271728-byte region
[0x7fac8f8fb800,0x7fad078fceb0)
allocated by thread T0 here:
    #0 0x4ae6f0 in malloc /home/bupt/Desktop/tools/llvm-12.0.1/llvm/projects/compiler-
rt/lib/asan/asan_malloc_linux.cpp:145
    #1 0x4f51ec in main /home/bupt/Desktop/PNGdec/linux/main.cpp:128:34

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/bupt/Desktop/PNGdec/linux/main.cpp:84:24 in
SaveBMP(char*, unsigned char*, unsigned char*, int, int, int)
Shadow bytes around the buggy address:
  0x0ff620f17980: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ff620f17990: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ff620f179a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ff620f179b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0ff620f179c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0ff620f179d0: 00 00 00 00 00 00[fa]fa fa fa fa fa fa fa fa fa
  0x0ff620f179e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
```

```
  0x0ff620f179f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff620f17a00: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff620f17a10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0ff620f17a20: 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
  Shadow gap:              cc
==23090==ABORTING
```

# stack-buffer-overflow

## crash sample No.1

id12-stack-buffer-overflow-sample1.zip

## crash info of sample No.1

```
==26778==ERROR: AddressSanitizer: stack-buffer-overflow on address 0x7ffc0d703c40 at pc
0x0000004f4e82 bp 0x7ffc0d702f90 sp 0x7ffc0d702f88
WRITE of size 1 at 0x7ffc0d703c40 thread T0
    #0 0x4f4e81 in SaveBMP(char*, unsigned char*, unsigned char*, int, int, int)
/home/bupt/Desktop/PNGdec/linux/main.cpp:84:48
    #1 0x4f5311 in main /home/bupt/Desktop/PNGdec/linux/main.cpp:144:9
    #2 0x7fd91072ac86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #3 0x41c129 in _start (/home/bupt/Desktop/PNGdec/linux/png_demo+0x41c129)

Address 0x7ffc0d703c40 is located in stack of thread T0 at offset 3232 in frame
    #0 0x4f425f in SaveBMP(char*, unsigned char*, unsigned char*, int, int, int)
/home/bupt/Desktop/PNGdec/linux/main.cpp:26

  This frame has 2 object(s):
```

```
    [32, 1056) 'ucTemp' (line 31)
    [1184, 3232) 'ucTemp76' (line 80) <== Memory access at offset 3232 overflows this variable
HINT: this may be a false positive if your program uses some custom stack unwind mechanism,
swapcontext or vfork
      (longjmp and C++ exceptions *are* supported)
SUMMARY: AddressSanitizer: stack-buffer-overflow /home/bupt/Desktop/PNGdec/linux/main.cpp:84:48 in
SaveBMP(char*, unsigned char*, unsigned char*, int, int, int)
Shadow bytes around the buggy address:
  0x100001ad8730: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100001ad8740: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100001ad8750: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100001ad8760: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100001ad8770: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x100001ad8780: 00 00 00 00 00 00 00 00[f3]f3 f3 f3 f3 f3 f3 f3
  0x100001ad8790: f3 f3 f3 f3 f3 f3 f3 f3 00 00 00 00 00 00 00 00
  0x100001ad87a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100001ad87b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100001ad87c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100001ad87d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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
==26778==ABORTING
```

# global-buffer-overflow

## crash sample

id13-global-buffer-overflow-sample1.zip

## crash info of the sample

```
==26922==ERROR: AddressSanitizer: global-buffer-overflow on address 0x00000101b510 at pc
0x00000051493d bp 0x7ffe4b62fc20 sp 0x7ffe4b62fc18
WRITE of size 1 at 0x00000101b510 thread T0
    #0 0x51493c in inflate_fast /home/bupt/Desktop/PNGdec/linux/../src/inffast.c:275:36
    #1 0x5180f8 in inflate /home/bupt/Desktop/PNGdec/linux/../src/inflate.c:1055:17
    #2 0x4f74e0 in DecodePNG(png_image_tag*, void*, int)
/home/bupt/Desktop/PNGdec/linux/../src/png.inl:783:31
    #3 0x4f74e0 in PNG::decode(void*, int)
/home/bupt/Desktop/PNGdec/linux/../src/PNGdec.cpp:194:12
    #4 0x4f5207 in main /home/bupt/Desktop/PNGdec/linux/main.cpp:129:18
    #5 0x7f5825c48c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #6 0x41c129 in _start (/home/bupt/Desktop/PNGdec/linux/png_demo+0x41c129)

0x00000101b510 is located 0 bytes to the right of global variable 'png' defined in 'main.cpp:10:5'
(0x100f8a0) of size 48240
SUMMARY: AddressSanitizer: global-buffer-overflow
/home/bupt/Desktop/PNGdec/linux/../src/inffast.c:275:36 in inflate_fast
Shadow bytes around the buggy address:
  0x0000801fb650: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0000801fb660: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0000801fb670: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0000801fb680: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0000801fb690: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0000801fb6a0: 00 00[f9]f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
  0x0000801fb6b0: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
  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
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
==26922==ABORTING
```

# memory allocation problem

## crash sample No.1

id5-memory-allocation-problem-sample1.zip

## crash info of sample No.1

```
==22984==ERROR: AddressSanitizer: requested allocation size 0xffffffff837c16b0 (0xffffffff837c26b0
after adjustments for alignment, red zones etc.) exceeds maximum supported size of 0x10000000000
(thread T0)
    #0 0x4ae6f0 in malloc /home/bupt/Desktop/tools/llvm-12.0.1/llvm/projects/compiler-
rt/lib/asan/asan_malloc_linux.cpp:145
    #1 0x4f51ec in main /home/bupt/Desktop/PNGdec/linux/main.cpp:128:34

==22984==HINT: if you don't care about these errors you may set allocator_may_return_null=1
SUMMARY: AddressSanitizer: allocation-size-too-big /home/bupt/Desktop/tools/llvm-
12.0.1/llvm/projects/compiler-rt/lib/asan/asan_malloc_linux.cpp:145 in malloc
==22984==ABORTING
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant