

New issue

[Jump to bottom](#)

heap-buffer-overflow found? #144

Open Cvjark opened this issue on Jun 1 · 0 comments

Assignees



Cvjark commented on Jun 1 • edited ▾

sample here:

[heap-bufferoverflow-pos-\)%at pdfalto.zip](#)

Describe info:

```
$ ./pdfalto heap-bufferoverflow-pos-)%at\ pdfalto.cc\:190\:5
```

```
==43072==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6040000000f1 at pc
0x00000043f92b bp 0x7fff65e8f0f0 sp 0x7fff65e8e8a0
WRITE of size 33 at 0x6040000000f1 thread T0
#0 0x43f92a in strncat /home/bupt/Desktop/tools/llvm-12.0.1/llvm/projects/compiler-
rt/lib/asan/asan_interceptors.cpp:397
#1 0x503603 in main /home/bupt/Desktop/pdfalto/src/pdfalto.cc:190:5
#2 0x7f8cfec7dc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
#3 0x422ca9 in _start (/home/bupt/Desktop/pdfalto/build/pdfalto+0x422ca9)
```

```
0x6040000000f1 is located 0 bytes to the right of 33-byte region [0x6040000000d0,0x6040000000f1)
allocated by thread T0 here:
```

```
#0 0x4b5270 in malloc /home/bupt//tools/llvm-12.0.1/llvm/projects/compiler-
rt/lib/asan/asan_malloc_linux.cpp:145
#1 0x5035f1 in main /home/bupt/Desktop/pdfalto/src/pdfalto.cc:189:22
#2 0x7f8cfec7dc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
```

```
SUMMARY: AddressSanitizer: heap-buffer-overflow /home/bupt//tools/llvm-
12.0.1/llvm/projects/compiler-rt/lib/asan/asan_interceptors.cpp:397 in strncat
```

Shadow bytes around the buggy address:

```
0x0c087fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c087fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c087fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c087fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c087fff8000: fa fa fd fd fd fd fd fa fa 00 00 00 00 00 04
```

```
=>0x0c087fff8010: fa fa 00 00 00 00 01 fa fa 00 00 00 00[01]fa
0x0c087fff8020: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c087fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c087fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c087fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c087fff8060: 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
==43072==ABORTING
```


  **kermitt2** self-assigned this on Jun 3

 **SchrodingersMind** added a commit to SchrodingersMind/pdfalto that referenced this issue on Aug 24 

 Fix [kermitt2#144](#) ...

94bff40

Assignees

 **kermitt2**

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

